An invitation to additive prime number theory

A. V. Kumchev and D. I. Tolev

March 31, 2007

Abstract

The main purpose of this survey is to introduce the inexperienced reader to additive prime number theory and some related branches of analytic number theory. We state the main problems in the field, sketch their history and the basic machinery used to study them, and try to give a representative sample of the directions of current research.

2000 MSC: 11D75, 11D85, 11L20, 11N05, 11N35, 11N36, 11P05, 11P32, 11P55.

1 Introduction

Additive number theory is the branch of number theory that studies the representations of natural numbers as sums of integers subject to various arithmetic restrictions. For example, given a sequence of integers

$$\mathcal{A} = \{a_1 < a_2 < a_3 < \cdots\}$$

one often asks what natural numbers can be represented as sums of a fixed number of elements of $\mathcal{A}$; that is, for any fixed $s \in \mathbb{N}$, one wants to find the natural numbers n such that the diophantine equation

$$x_1 + \cdots + x_s = n \tag{1.1}$$

has a solution in $x_1, \dots, x_s \in \mathcal{A}$. The sequence $\mathcal{A}$ may be described in some generality (say, one may assume that $\mathcal{A}$ contains "many" integers), or it may be a particular sequence of some arithmetic interest (say, $\mathcal{A}$ may be the sequence of kth powers, the sequence of prime numbers, the values taken by a polynomial $F(X) \in \mathbb{Z}[X]$ at the positive integers or at the primes, etc.). In this survey, we discuss almost exclusively problems of the latter kind. The main focus will be on two questions, known as Goldbach's problem and the Waring–Goldbach problem, which are concerned with representations as sums of primes and powers of primes, respectively.

1.1 Goldbach's problem

Goldbach's problem appeared for the first time in 1742 in the correspondence between Goldbach and Euler. In modern language, it can be stated as follows.

Goldbach's Conjecture. *Every even integer $n \geq 4$ is the sum of two primes, and every odd integer $n \geq 7$ is the sum of three primes.*

The two parts of this conjecture are known as the binary Goldbach problem and the ternary Goldbach problem, respectively. Clearly, the binary conjecture is the stronger one. It is also much more difficult.

The first theoretical evidence in support of Goldbach's conjecture was obtained by Brun [27], who showed that every large even integer is the sum of two integers having at most nine prime factors. Brun also obtained an upper bound of the correct order for the number of representations of a large even integer as the sum of two primes.

During the early 1920s Hardy and Littlewood [67]–[72] developed the ideas in an earlier paper by Hardy and Ramanujan [73] into a new analytic method in additive number theory. Their method is known as the *circle method*. In 1923 Hardy and Littlewood [69, 71] applied the circle method to Goldbach's problem. Assuming the Generalized Riemann Hypothesis[1] (GRH), they proved that all but finitely many odd integers are sums of three primes and that all but $O\left(x^{1/2+\varepsilon}\right)$ even integers $n \leq x$ are sums of two primes. (Henceforth, ε denotes a positive number which can be chosen arbitrarily small if the implied constant is allowed to depend on ε.)

During the 1930s Schnirelmann [201] developed a probabilistic approach towards problems in additive number theory. Using his method and Brun's results, he was able to prove unconditionally that there exists a positive integer s such that every sufficiently large integer is the sum of at most s primes. Although the value of s arising from this approach is much larger than the conjectured $s = 3$, Schnirelmann's result represented a significant achievement, as it defeated the popular belief at the time that the solution of Goldbach's problem must depend on GRH. (Since its first appearance, Schnirelmann's method has been polished significantly. In particular, the best result to date obtained in this fashion by Ramare [193] states that one can take $s = 7$.)

In 1937 I. M. Vinogradov [236] found an ingenious new method for estimating sums over primes, which he applied to the exponential sum

$$f(\alpha) = \sum_{p \leq n} e(\alpha p), \tag{1.2}$$

where α is real, p denotes a prime, and $e(\alpha) = \exp(2\pi i\alpha)$. Using his estimate for $f(\alpha)$, Vinogradov was able to give a new, unconditional proof of the result of Hardy and Littlewood on the ternary Goldbach problem. His result is known as Vinogradov's three prime theorem.

Theorem 1 (Vinogradov, 1937). *For a positive integer n, let $R(n)$ denote the number of representations of n as the sum of three primes. Then*

$$R(n) = \frac{n^2}{2(\log n)^3}\mathfrak{S}(n) + O\left(n^2(\log n)^{-4}\right), \tag{1.3}$$

[1] An important conjecture about certain Dirichlet series; see §2.2 for details.

where

$$\mathfrak{S}(n) = \prod_{p|n} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p\nmid n} \left(1 + \frac{1}{(p-1)^3}\right). \tag{1.4}$$

In particular, every sufficiently large odd integer is the sum of three primes.

The products in (1.4) are over the primes dividing n and over those not dividing n, respectively. In particular, when n is even, we have $\mathfrak{S}(n) = 0$, making (1.3) trivial. On the other hand, when n is odd, we have $\mathfrak{S}(n) \geq 1$. We describe the proof of Theorem 1 in §3.1.

It should be noted that the independence of GRH in Theorem 1 comes at the price of a mind-boggling implied constant. If one avoids O-notation and makes all the constants explicit, one finds that the original (GRH-dependent) work of Hardy and Littlewood establishes the ternary Goldbach conjecture for $n \geq 10^{50}$, whereas Vinogradov's method requires $n \geq 10^{6\,800\,000}$ and even its most refined version available today (see Liu and Wang [163]) requires $n \geq 10^{1\,346}$. To put these numbers in perspective, we remark that even the bound 10^{50} is beyond hope of "checking the remaining cases by a computer". In fact, only recently have Deshouillers *et al.* [51] proved that if GRH is true, the ternary Goldbach conjecture holds for all odd $n \geq 7$.

In 1938, using Vinogradov's method, Chudakov [42], van der Corput [43], and Estermann [54] each showed that *almost all* even integers $n \leq x$ are sums of two primes. More precisely, they proved that for any $A > 0$ we have

$$E(x) = O\left(x(\log x)^{-A}\right), \tag{1.5}$$

where $E(x)$ denotes the number of even integers $n \leq x$ that cannot be represented as the sum of two primes. The first improvement on (1.5) was obtained by Vaughan [220]. It was followed by a celebrated work by Montgomery and Vaughan [173] from 1975, in which they established the existence of an absolute constant $\delta > 0$ such that

$$E(x) = O\left(x^{1-\delta}\right). \tag{1.6}$$

The first to compute an explicit numerical value for δ were Chen and Pan [36]. They showed that the method of Montgomery and Vaughan yields (1.6) with $\delta = 0.01$. Subsequently, this result has been sharpened by several authors and currently (1.6) is known to hold with $\delta = 0.086$ (see Li [136]). In June 2004, Pintz [186] announced a further improvement on (1.6). He has established the above bound with $\delta = \frac{1}{3}$ and can also show that for all but $O(x^{3/5+\varepsilon})$ even integers $n \leq x$ either n or $n-2$ is the sum of two primes.

One may also think of the binary Goldbach conjecture as a claim about the primes in the sequence

$$\mathcal{A} = \mathcal{A}(n) = \{n - p : p \text{ prime number},\ 2 < p < n\}, \tag{1.7}$$

namely, that such primes exist for all even $n \geq 6$. Denote by P_r an integer having at most r prime factors, counted with their multiplicities, and refer to such a number as an *almost*

prime of order r (thus, Brun's result mentioned above asserts that every large even n can be represented in the form $n = P_9 + P_9'$). In 1947 Rényi [195] proved that there is a fixed integer r such that the sequence $\mathcal{A}$ contains a P_r-number when n is sufficiently large. Subsequent work by many mathematicians reduced the value of r in Rényi's result almost to the possible limit and fell just short of proving the binary Goldbach conjecture. The best result to date was obtained by Chen [35].

Theorem 2 (Chen, 1973). *For an even integer n, let $r(n)$ denote the number of representations of n in the form $n = p + P_2$, where p is a prime and P_2 is an almost prime of order 2. There exists an absolute constant n_0 such that if $n \geq n_0$, then*

$$r(n) > 0.67 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p>2 \\ p|n}} \left(\frac{p-1}{p-2}\right) \frac{n}{(\log n)^2}.$$

In particular, every sufficiently large even integer n can be represented in the form $n = p + P_2$.

1.2 Waring's problem

Before proceeding with the Waring–Goldbach problem, we will make a detour to present the most important results in Waring's problem, as those results and the work on Goldbach's problem have been the main motivation behind the Waring–Golbach problem. It was probably the ancient Greeks who first observed that every positive integer is the sum of four integer squares, but it was not until 1770 that a complete proof of this remarkable fact was given by Lagrange. Also in 1770, Waring proposed a generalization of the four square theorem that became known as Waring's problem and arguably led to the emergence of additive number theory. In modern terminology, Waring's conjecture states that for every integer $k \geq 2$ there exists an integer $s = s(k)$ such that every natural number n is the sum of at most s kth powers of natural numbers. Several special cases of this conjecture were settled during the 19th century, but the complete solution eluded mathematicians until 1909, when Hilbert [95] proved the existence of such an s for all k by means of a difficult combinatorial argument.

Let $g(k)$ denote the least possible s as above. Hilbert's method produced a very poor bound for $g(k)$. Using the circle method, Hardy and Littlewood were able to improve greatly on Hilbert's bound for $g(k)$. In fact, through the efforts of many mathematicians, the circle method in conjunction with elementary and computational arguments has led to a nearly complete evaluation of $g(k)$. In particular, we know that $g(k)$ is determined by certain special integers $n < 4^k$ that can only be represented as sums of a large number of kth powers of 1, 2 and 3 (see [228, §1.1] for further details on $g(k)$).

A much more difficult question, and one that leads to a much deeper understanding of the additive properties of kth powers, is that of estimating the function $G(k)$, defined as the least s such that every *sufficiently large* positive integer n is the sum of s kth powers. This function was introduced by Hardy and Littlewood [70], who obtained the bound

$$G(k) \leq (k-2)2^{k-1} + 5. \tag{1.8}$$

In fact, they proved more than that. Let $I_{k,s}(n)$ denote the number of solutions of the diophantine equation

$$x_1^k + x_2^k + \cdots + x_s^k = n \tag{1.9}$$

in $x_1, \ldots, x_s \in \mathbb{N}$. Hardy and Littlewood showed that if $s \geq (k-2)2^{k-1} + 5$, then

$$I_{k,s}(n) \sim \frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)} \mathfrak{S}_{k,s}(n) n^{s/k-1} \qquad \text{as} \quad n \to \infty, \tag{1.10}$$

where Γ stands for Euler's gamma-function and $\mathfrak{S}_{k,s}(n)$ is an absolutely convergent infinite series, called the *singular series*, such that

$$\mathfrak{S}_{k,s}(n) \geq c_1(k,s) > 0.$$

While the upper bound (1.8) represents a tremendous improvement over Hilbert's result, it is still quite larger than the trivial lower bound $G(k) \geq k+1$.[2] During the mid-1930s I. M. Vinogradov introduced several refinements of the circle method that allowed him to obtain a series of improvements on (1.8) for large k. In their most elaborate version, Vinogradov's methods yield a bound of the form[3]

$$G(k) \leq 2k(\log k + O(\log\log k)).$$

First published by Vinogradov [240] in 1959, this bound withstood any significant improvement until 1992, when Wooley [245] proved that

$$G(k) \leq k(\log k + \log\log k + O(1)).$$

The latter is the sharpest bound to date for $G(k)$ when k is large. For smaller k, one can obtain better results by using more specialized techniques (usually refinements of the circle method). The best known bounds for $G(k)$, $3 \leq k \leq 20$, are of the form $G(k) \leq F(k)$, with $F(k)$ given by Table 1 below.

k	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$F(k)$	7	16	17	24	33	42	50	59	67	76	84	92	100	109	117	125	134	142

TABLE 1. Bounds for $G(k)$, $3 \leq k \leq 20$.

[2]Let X be large. If $n \leq X$, any solution of (1.9) must satisfy $1 \leq x_1, \ldots, x_s \leq X^{1/k}$. There at most $X^{s/k}$ such s-tuples, which yield at most $(1/s! + o(1))X^{s/k}$ distinct sums $x_1^k + \cdots + x_s^k$. Thus, when $s \leq k$, there are not enough sums of s kth powers to represent all the integers.

[3]In this and similar results appearing later, one can obtain an explicit expressions in place of the O-terms, but those are too complicated to state here.

With the exception of the bound $G(3) \le 7$, all of these results have been obtained by an iterative version of the circle method that originated in the work of Davenport [46, 48] and Davenport and Erdös [50]. The bound for $G(3)$ was established first by Linnik [141] and until recently lay beyond the reach of the circle method. The result on $G(4)$ is due to Davenport [47], and in fact states that $G(4) = 16$. This is because 16 biquadrates are needed to represent integers of the form $n = 31 \cdot 16^r$, $r \in \mathbb{N}$. Other than Lagrange's four squares theorem, this is the only instance in which the exact value of $G(k)$ is known. However, Davenport [47] also proved that if $s \ge 14$, all sufficiently large integers $n \equiv r \pmod{16}$, $1 \le r \le s$, can be written as the sum of s biquadrates; Kawada and Wooley [120] obtained a similar result for as few as 11 biquadrates. The remaining bounds in Table 1 appear in a series of recent papers by Vaughan and Wooley [229]–[232].

A great deal of effort has also been dedicated to estimating the function $\tilde{G}(k)$, which represents the least s for which the asymptotic formula (1.10) holds. For large k, Ford [57] showed that

$$\tilde{G}(k) \le k^2(\log k + \log\log k + O(1)), \tag{1.11}$$

thus improving on earlier work by Vinogradov [238], Hua [101], and Wooley [246]. Furthermore, Vaughan [226, 227] and Boklan [18] obtained the bounds

$$\tilde{G}(k) \le 2^k \quad (k \ge 3) \qquad \text{and} \qquad \tilde{G}(k) \le \tfrac{7}{8} \cdot 2^k \quad (k \ge 6),$$

which supersede (1.11) when $k \le 8$.

The work on Waring's problem has inspired research on several other questions concerned with the additive properties of kth powers (and of more general polynomial sequences). Such matters, however, are beyond the scope of this survey. The reader interested in a more comprehensive introduction to Waring's problem should refer to the monographs [4, 228] or to a recent survey article by Vaughan and Wooley [233] (the latter also provides an excellent account of the history of Waring's problem).

1.3 The Waring–Goldbach problem

Vinogradov's proof of the three prime theorem provided a blueprint for subsequent applications of the Hardy–Littlewood circle method to additive problems involving primes. Shortly after the publication of Theorem 1, Vinogradov himself [237] and Hua [100] began studying Waring's problem with prime variables, known nowadays as the *Waring–Goldbach problem*. They were able to generalize the asymptotic formula (1.3) to kth powers for all $k \ge 1$ and ultimately their efforts led to the proof of Theorem 3 below.

In order to describe the current knowledge about the Waring–Goldbach problem, we first need to introduce some notation. Let k be a positive integer and p a prime. We denote by $\theta = \theta(k,p)$ the (unique) integer such that $p^\theta \mid k$ and $p^{\theta+1} \nmid k$, and then define

$$\gamma = \gamma(k,p) = \begin{cases} \theta + 2, & \text{if } p = 2,\ 2 \mid k, \\ \theta + 1, & \text{otherwise,} \end{cases} \qquad K(k) = \prod_{(p-1)\mid k} p^\gamma. \tag{1.12}$$

In particular, we have $K(1) = 2$. It is not difficult to show that if an integer n is the sum of s kth powers of primes greater than $k+1$, then n must satisfy the congruence condition $n \equiv s \pmod{K(k)}$. Furthermore, define

$$S(q,a) = \sum_{\substack{h=1\\(h,q)=1}}^{q} e\left(\frac{ah^k}{q}\right), \quad \mathfrak{S}^*_{k,s}(n) = \sum_{q=1}^{\infty} \sum_{\substack{a=1\\(a,q)=1}}^{q} \frac{S(q,a)^s}{\phi(q)^s} e\left(\frac{-an}{q}\right), \tag{1.13}$$

where (a,q) stands for the greatest common divisor of a and q, and $\phi(q)$ is Euler's totient function, that is, the number of positive integers $n \le q$ which are relatively prime to q. The following result will be established in §3.3 and §3.4.

Theorem 3. *Let k, s and n be positive integers, and let $R^*_{k,s}(n)$ denote the number of solutions of the diophantine equation*

$$p_1^k + p_2^k + \cdots + p_s^k = n \tag{1.14}$$

in primes $p_1, \ldots, p_s$. Suppose that

$$s \ge \begin{cases} 2^k + 1, & \text{if } \ 1 \le k \le 5, \\ \frac{7}{8} \cdot 2^k + 1, & \text{if } \ 6 \le k \le 8, \\ k^2(\log k + \log\log k + O(1)), & \text{if } \ k > 8. \end{cases}$$

Then

$$R^*_{k,s}(n) \sim \frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)} \mathfrak{S}^*_{k,s}(n) \frac{n^{s/k-1}}{(\log n)^s} \qquad \text{as} \quad n \to \infty, \tag{1.15}$$

where $\mathfrak{S}^*_{k,s}(n)$ is defined by (1.13). *Furthermore, the singular series $\mathfrak{S}^*_{k,s}(n)$ is absolutely convergent, and if $n \equiv s \pmod{K(k)}$, then $\mathfrak{S}^*_{k,s}(n) \ge c_2(k,s) > 0$.*

In particular, we have the following corollaries to Theorem 3.

Corollary 3.1. *Every sufficiently large integer $n \equiv 5 \pmod{24}$ can be represented as the sum of five squares of primes.*

Corollary 3.2. *Every sufficiently large odd integer can be represented as the sum of nine cubes of primes.*

Hua introduced a function $H(k)$ similar to the function $G(k)$ in Waring's problem. $H(k)$ is defined as the least integer s such that equation (1.14) has a solution in primes $p_1, \ldots, p_s$ for all sufficiently large $n \equiv s \pmod{K(k)}$. It is conjectured that $H(k) = k+1$ for all $k \ge 1$, but this conjecture has not been proved for any value of k yet. When $k \le 3$, the sharpest known upper bounds for $H(k)$ are those given by Theorem 3, that is,

$$H(1) \le 3, \quad H(2) \le 5, \quad H(3) \le 9.$$

When $k \ge 4$, the best results in the literature are as follows.

Theorem 4. *Let $k \geq 4$ be an integer, and let $H(k)$ be as above. Then*

$$H(k) \leq \begin{cases} F(k), & \text{if} \quad 4 \leq k \leq 10, \\ k(4\log k + 2\log\log k + O(1)), & \text{if} \quad k > 10, \end{cases}$$

where $F(k)$ is given by the following table.

k	4	5	6	7	8	9	10
$F(k)$	14	21	33	46	63	83	107

TABLE 2. Bounds for $H(k)$, $4 \leq k \leq 10$.

The cases $k = 6$ and $8 \leq k \leq 10$ of Theorem 4 are due to Thanigasalam [211], and the cases $k = 4, 5$ and 7 are recent results of Kawada and Wooley [121] and Kumchev [127], respectively. The bound for $k > 10$ is an old result of Hua, whose proof can be found in Hua's book [102]. To the best of our knowledge, this is the strongest published result for large k, although it is well-known to experts in the field that better results are within the reach of Wooley's refinement of Vinogradov's methods. In particular, by inserting Theorem 1 in Wooley [247] into the machinery developed in Hua's monograph, one obtains

$$H(k) \leq k(\tfrac{3}{2}\log k + O(\log\log k)) \qquad \text{for} \quad k \to \infty.$$

1.4 Other additive problems involving primes

There are several variants and generalizations of the Waring–Goldbach problem that have attracted a lot of attention over the years. For example, one may consider the diophantine equation

$$a_1 p_1^k + a_2 p_2^k + \cdots + a_s p_s^k = n, \tag{1.16}$$

where $n, a_1, \ldots, a_s$ are fixed, not necessarily positive, integers. There are several questions that we can ask about equations of this form. The main question, of course, is that of solubility. Furthermore, in cases where we do know that (1.16) is soluble, we may want to count the solutions with $p_1, \ldots, p_s \leq X$, where X is a large parameter. A famous problem of this type is the *twin-prime conjecture*: there exist infinitely many primes p such that $p + 2$ is also prime, that is, the equation

$$p_1 - p_2 = 2$$

has infinitely many solutions. It is believed that this conjecture is of the same difficulty as the binary Goldbach problem, and in fact, the two problems share a lot of common history. In particular, while the twin-prime conjecture is still open, Chen's proof of Theorem 2 can be easily modified to establish that there exist infinitely many primes p such that $p+2 = P_2$.

Other variants of the Waring–Goldbach problem consider more general diophantine equations of the form

$$f(p_1) + f(p_2) + \cdots + f(p_s) = n,$$

where $f(X) \in \mathbb{Z}[X]$, or systems of equations of the types (1.1) or (1.16). For example, Chapters 10 and 11 in Hua's monograph [102] deal with the system

$$p_1^j + p_2^j + \cdots + p_s^j = n_j \qquad (1 \le j \le k).$$

The number of solutions of this system satisfies an asymptotic formula similar to (1.15), but the main term in that asymptotic formula is less understood than the main term in (1.15) (see [3, 41, 102, 170] for further details).

Another classical problem in which a system of diophantine equations arises naturally concerns the existence of non-trivial arithmetic progressions consisting of r primes. It has been conjectured that for every integer $r \ge 3$ there are infinitely many such arithmetic progressions. In other words, the linear system

$$p_i - 2p_{i+1} + p_{i+2} = 0 \qquad (1 \le i \le r-2)$$

has infinitely many solutions in distinct primes $p_1, \dots, p_r$. In the case $r = 3$ this can be established by a variant of Vinogardov's proof of the three primes theorem, but when $r > 3$ the above system lies beyond the reach of the circle method. In fact, until recently the most significant insight into progressions of more than three primes were the following two results:

- Heath-Brown [83] succeeded to prove that there exist infinitely many arithmetic progressions of three primes and a P_2-number.
- Balog [11] proved that for any r there are r distinct primes $p_1, \dots, p_r$ such that all the averages $\frac{1}{2}(p_i + p_j)$ are prime.

Thus, the specialists in the field were stunned when Green and Tao [64] announced their amazing proof of the full conjecture. The reader will find a brief description of their ideas and of some related recent work in the last section.

Finally, instead of (1.1), one may study the inequality

$$|x_1 + \cdots + x_s - \alpha| < \varepsilon,$$

where α is a real number, ε is a small positive number and $x_1, \dots, x_s$ are real variables taking values from a given sequence (or sequences). For example, by setting $x_j = p_j^c$ where $c > 1$ in not an integer, we can generalize the Waring–Goldbach problem to fractional powers of primes. We will mention several results of this form in §5.7.

2 The distribution of primes

In this section we discuss briefly some classical results about primes, which play an important role in additive prime number theory.

2.1 The Prime Number Theorem

The first result on the distribution of primes is Euclid's theorem that there are infinitely many prime numbers. In 1798 Legendre conjectured that the prime counting function $\pi(x)$ (i.e., the number of primes $p \le x$) satisfies the asymptotic relation

$$\lim_{x\to\infty} \frac{\pi(x)}{x/(\log x)} = 1; \tag{2.1}$$

this is the classical statement of the Prime Number Theorem. Later Gauss observed that the logarithmic integral

$$\operatorname{li} x = \int_2^x \frac{dt}{\log t}$$

seemed to provide a better approximation to $\pi(x)$ than the function $x/(\log x)$ appearing in (2.1), and this is indeed the case. Thus, in anticipation of versions of the Prime Number Theorem that are more precise than (2.1), we define the error term

$$\Delta(x) = \pi(x) - \operatorname{li} x. \tag{2.2}$$

The first step toward a proof of the Prime Number Theorem was made by Chebyshev. In the early 1850s he proved that (2.1) predicts correctly the order of $\pi(x)$, that is, he established the existence of absolute constants $c_2 > c_1 > 0$ such that

$$\frac{c_1 x}{\log x} \le \pi(x) \le \frac{c_2 x}{\log x}.$$

Chebyshev also showed that if the limit on the left side of (2.1) exists, then it must be equal to 1.

In 1859 Riemann published his famous memoir [197], in which he demonstrated the intimate relation between $\pi(x)$ and the function which now bears his name, that is, the *Riemann zeta-function* defined by

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p \left(1 - p^{-s}\right)^{-1} \quad (\operatorname{Re}(s) > 1). \tag{2.3}$$

This and similar series had been used earlier by Euler[4] and Dirichlet, but only as functions of a real variable. Riemann observed that $\zeta(s)$ is holomorphic in the half-plane $\operatorname{Re}(s) > 1$ and that it can be continued analytically to a meromorphic function, whose only singularity is a simple pole at $s = 1$. It is not difficult to deduce from (2.3) that $\zeta(s) \neq 0$ in the half-plane $\operatorname{Re}(s) > 1$. Riemann observed that $\zeta(s)$ has infinitely many zeros in the strip $0 \le \operatorname{Re}(s) \le 1$ and proposed several conjectures concerning those zeros and the relation between them and the Prime Number Theorem. The most famous among those conjecture—and the only one that is still open—is known as the *Riemann Hypothesis*.

[4]In particular, Euler established the equality between $\zeta(s)$ and the infinite product in (2.3), which is known as the *Euler product* of $\zeta(s)$.

Riemann Hypothesis (RH). *All the zeros of* $\zeta(s)$ *with* $0 \le \mathrm{Re}(s) \le 1$ *lie on the line* $\mathrm{Re}(s) = \frac{1}{2}$.

The remaining conjectures in Riemann's paper were proved by the end of the 19th century. In particular, it was proved that the Prime Number Theorem follows from the nonvanishing of $\zeta(s)$ on the line $\mathrm{Re}(s) = 1$. Thus, when in 1896 Hadamard and de la Vallée Poussin proved (independently) that $\zeta(1 + it) \neq 0$ for all real t, the Prime Number Theorem was finally proved. In 1899 de la Vallée Poussin obtained the following quantitative result.[5] (Henceforth, we often use Vinogradov's notation $A \ll B$, which means that $A = O(B)$.)

Theorem 5 (de la Vallée Poussin, 1899). *Let* $\Delta(x)$ *be defined by* (2.2). *There exists an absolute constant* $c > 0$ *such that*

$$\Delta(x) \ll x \exp\big(-c\sqrt{\log x}\big).$$

De la Vallée Poussin's theorem has been improved somewhat, but not nearly as much as one would hope. The best result to date is due to I. M. Vinogradov [239] and Korobov [123], who obtained (independently) the following estimate for $\Delta(x)$.

Theorem 6 (Vinogradov, Korobov, 1958). *Let* $\Delta(x)$ *be defined by* (2.2). *There exists an absolute constant* $c > 0$ *such that*

$$\Delta(x) \ll x \exp\big(-c(\log x)^{3/5}(\log\log x)^{-1/5}\big).$$

In comparison, if the Riemann Hypothesis is assumed, one has

$$\Delta(x) \ll x^{1/2} \log x, \tag{2.4}$$

which, apart from the power of the logarithm, is best possible. The reader can find further information about the Prime Number Theorem and the Riemann zeta-function in the standard texts on the subject (e.g., [49, 103, 117, 191, 212]).

2.2 Primes in arithmetic progressions

In a couple of memoirs published in 1837 and 1840, Dirichlet proved that if a and q are natural numbers with $(a, q) = 1$, then the arithmetic progression $a \bmod q$ contains infinitely many primes. In fact, Dirichlet's argument can be refined as to establish the asymptotic formula

$$\sum_{\substack{p \le x \\ p \equiv a \pmod q}} \frac{\log p}{p} \sim \frac{1}{\phi(q)} \sum_{p \le x} \frac{\log p}{p} \qquad \text{as} \quad x \to \infty, \tag{2.5}$$

[5] Functions of the type $f(x) = \exp\big((\log x)^\lambda\big)$, where λ is a constant, are quite common in analytic number theory. To help the reader appreciate results such as Theorems 5 and 6, we remark that as $x \to \infty$ such a function with $0 < \lambda < 1$ grows more rapidly than any fixed power of $\log x$, but less rapidly than x^ε for any fixed $\varepsilon > 0$.

valid for all a and q with $(a,q)=1$. Fix q and consider the various arithmetic progressions $a \bmod q$ (here $\phi(q)$ is Euler's totient function). Since all but finitely many primes lie in progressions with $(a,q)=1$ and there are $\phi(q)$ such progressions, (2.5) suggests that each arithmetic progression $a \bmod q$, with $(a,q)=1$, "captures its fair share" of prime numbers, i.e., that the primes are uniformly distributed among the (appropriate) arithmetic progressions to a given modulus q. Thus, one may expect that if $(a,q)=1$, then

$$\pi(x;q,a) = \sum_{\substack{p\le x\\ p\equiv a \pmod q}} 1 \sim \frac{\operatorname{li} x}{\phi(q)} \qquad \text{as} \quad x\to\infty. \tag{2.6}$$

This is the *prime number theorem for arithmetic progressions*. One may consider (2.6) from two different view points. First, one may fix a and q and ask whether (2.6) holds (allowing the convergence to depend on q and a). Posed in this form, the problem is a minor generalization of the Prime Number Theorem. In fact, shortly after proving Theorem 5, de la Vallée Poussin established that

$$\Delta(x;q,a) = \pi(x;q,a) - \frac{\operatorname{li} x}{\phi(q)} \ll x\exp\big(-c\sqrt{\log x}\big),$$

where $c=c(q,a)>0$ and the implied constant depends on q and a. The problem becomes much more difficult if one requires an estimate that is explicit in q and uniform in a. The first result of this kind was obtained by Page [176], who proved the existence of a (small) positive number δ such that

$$\Delta(x;q,a) \ll x\exp\big(-(\log x)^{\delta}\big), \tag{2.7}$$

whenever $1\le q\le (\log x)^{2-\delta}$ and $(a,q)=1$. In 1935 Siegel [208] (essentially) proved the following result known as the Siegel–Walfisz theorem.

Theorem 7 (Siegel, 1935). *For any fixed $A>0$, there exists a constant $c=c(A)>0$ such that*

$$\pi(x;q,a) = \frac{\operatorname{li} x}{\phi(q)} + O\big(x\exp\big(-c\sqrt{\log x}\big)\big)$$

whenever $q\le(\log x)^A$ and $(a,q)=1$.

Remark. While this result is clearly sharper than Page's, it does have one significant drawback: it is ineffective, that is, given a particular value of A, the proof does not allow the constant $c(A)$ or the O-implied constant to be computed.

The above results have been proved using the analytic properties of a class of generalizations of the Riemann zeta-function known as *Dirichlet L-functions*. For each positive integer q there are $\phi(q)$ functions $\chi:\mathbb{Z}\to\mathbb{C}$, called *Dirichlet characters* mod q, with the following properties:

- χ is *totally multiplicative*: $\chi(mn)=\chi(m)\chi(n)$;

- χ is q-periodic;
- $|\chi(n)| = 1$ if $(n, q) = 1$ and $\chi(n) = 0$ if $(n, q) > 1$;
- if $(n, q) = 1$, then

$$\sum_{\chi \bmod q} \chi(n) = \begin{cases} \phi(q) & \text{if } \ n \equiv 1 \pmod{q}, \\ 0 & \text{otherwise.} \end{cases}$$

For more information about the construction and properties of the Dirichlet characters we refer the reader to [49, 108, 116, 191].

Given a character $\chi \bmod q$, we define the Dirichlet L-function

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = \prod_{p} \left(1 - \chi(p) p^{-s}\right)^{-1} \quad (\mathrm{Re}(s) > 1).$$

Similarly to $\zeta(s)$, $L(s, \chi)$ is holomorphic in the half-plane $\mathrm{Re}(s) > 1$ and can be continued analytically to a meromorphic function on $\mathbb{C}$ that has at most one pole, which (if present) must be a simple pole at $s = 1$. Furthermore, just as $\zeta(s)$, the continued $L(s, \chi)$ has infinitely many zeros in the strip $0 \le \mathrm{Re}(s) \le 1$, and the horizontal distribution of those zeros has important implications on the distribution of primes in arithmetic progressions. For example, the results of de la Vallée Poussin, Page and Siegel mentioned above were proved by showing that no L-function can have a zero "close" to the line $\mathrm{Re}(s) = 1$. We also have the following generalization of the Riemann Hypothesis.

Generalized Riemann Hypothesis (GRH). *Let $L(s, \chi)$ be a Dirichlet L-function. Then all the zeros of $L(s, \chi)$ with $0 \le \mathrm{Re}(s) \le 1$ lie on the line $\mathrm{Re}(s) = \frac{1}{2}$.*

Assuming GRH, we can deduce easily that if $(a, q) = 1$, then

$$\pi(x; q, a) = \frac{\operatorname{li} x}{\phi(q)} + O\left(x^{1/2} \log x\right), \tag{2.8}$$

which is nontrivial when $1 \le q \le x^{1/2} (\log x)^{-2-\varepsilon}$.

In many applications one only needs (2.8) to hold "on average" over the moduli q. During the 1950s and 1960s several authors obtained estimates for averages of $\Delta(x; q, a)$. In particular, the following quantity was studied extensively:

$$E(x, Q) = \sum_{q \le Q} \max_{(a,q)=1} \max_{y \le x} |\Delta(y; q, a)|.$$

The trivial bound for this quantity is $E(x, Q) \ll x \log x$. One usually focuses on finding the largest value of Q for which one can improve on this trivial bound, even if the improvement is fairly modest. The sharpest result in this direction was established (independently) by Bombieri [19] and A. I. Vinogradov [234] in 1965. Their result is known as the Bombieri–Vinogradov theorem and (in the slightly stronger form given by Bombieri) can be stated as follows.

Theorem 8 (Bombieri, Vinogradov, 1965). *For any fixed $A > 0$, there exists a $B = B(A) > 0$ such that*

$$E(x, Q) \ll x(\log x)^{-A}, \tag{2.9}$$

provided that $Q \le x^{1/2}(\log x)^{-B}$.

We should note that other than the value of $B(A)$ the range for Q in this result is as long as the range we can deduce from GRH. Indeed, GRH yields $B = A + 1$, whereas Bombieri obtained Theorem 8 with $B = 3A + 22$ and more recently Vaughan [223] gave $B = A + 5/2$.

2.3 Primes in short intervals

Throughout this section, we write p_n for the nth prime number. We are interested in estimates for the difference $p_{n+1} - p_n$ between two consecutive primes. Cramér was the first to study this question systematically. He proved [44] that the Riemann Hypothesis implies

$$p_{n+1} - p_n \ll p_n^{1/2} \log p_n.$$

Cramér also proposed a probabilistic model of the prime numbers that leads to very precise (and very bold) predictions of the asymptotic properties of the primes. In particular, he conjectured [45] that

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log^2 p_n} = 1. \tag{2.10}$$

A non-trivial upper bound for $p_{n+1} - p_n$ can be obtained as a consequence of the Prime Number Theorem, but Hoheisel [96] found a much sharper result. He proved unconditionaly the asymptotic formula

$$\pi(x + h) - \pi(x) \sim h(\log x)^{-1} \qquad \text{as} \quad x \to \infty, \tag{2.11}$$

with $h = x^{1-(3300)^{-1}}$. There have been several improvements on Hoheisel's result and it is now known that (2.11) holds with $h = x^{7/12}$ (see Heath-Brown [86]). Furthermore, several mathematicians have shown that even shorter intervals must contain primes (without establishing an asymptotic formula for the number of primes in such intervals). The best result in this directions is due to Baker, Harman, and Pintz [9], who proved that for each n one has

$$p_{n+1} - p_n \ll p_n^{0.525}.$$

A related problem seeks small gaps between consecutive primes. In particular, the twin-prime conjecture can be stated in the form

$$\liminf_{n\to\infty} (p_{n+1} - p_n) = 2.$$

It is an exercise to show that the Prime Number Theorem implies the inequality

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} \le 1.$$

Improvements on this trivial bound, on the other hand, have proved notoriously difficult and, so far, the best result, due to Maier [165], is

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} \le 0.2486\ldots.$$

2.4 Primes in sparse sequences

We say that an infinite sequence of primes $\mathcal{S}$ is *sparse* if

$$\pi(\mathcal{S};x) := \#\big\{p\in\mathcal{S} : p\le x\big\} = o(\pi(x)) \qquad \text{as} \quad x\to\infty.$$

A classical example that has attracted a great deal of attention but has proved notoriously difficult is that of primes represented by polynomials. To this day, there is not a single example of a polynomial $f(X)\in\mathbb{Z}[X]$ of degree at least 2 which is known to take on infinitely many prime values. The closest approximation is a result of Iwaniec [104], who showed that if a,b,c are integers such that $a>0$, $(c,2)=1$, and the polynomial $f(X)=aX^2+bX+c$ is irreducible, then $f(X)$ takes on infinitely many P_2-numbers. On the other hand, in recent years there has been some exciting progress in the direction of finding polynomials in two variables that represent infinitely many primes. In 1998 Friedlander and Iwaniec [58] proved that the polynomial X^2+Y^4 represents infinitely many primes. We note that this polynomial takes on $O(x^{3/4})$ values up to x. In 2001 Heath-Brown [89] obtained an analogous result for the polynomial X^3+2Y^3 whose values are even sparser: it takes on $O(x^{2/3})$ values up to x. Furthermore, Heath-Brown and Moroz [92] extended the latter result to general irreducible binary cubic forms in $\mathbb{Z}[X,Y]$ (subject to some mild necessary conditions).

Another class of sparse sequences of prime numbers arises in the context of diophantine approximation. The two best known examples of this kind are the sequences

$$\mathcal{S}_\lambda = \big\{p : p \text{ is prime with } \{\sqrt{p}\} < p^{-\lambda}\big\} \tag{2.12}$$

and

$$\mathcal{P}_c = \{p : p=[n^c] \text{ for some integer } n\}. \tag{2.13}$$

Here, $\lambda\in(0,1)$ and $c>1$ are fixed real numbers, $\{x\}$ denotes the fractional part of the real number x, and $[x]=x-\{x\}$. The sequence $\mathcal{S}_\lambda$ was introduced by I. M. Vinogradov, who proved (see [241, Chapter 4]) that if $0<\lambda<1/10$, then

$$\pi(\mathcal{S}_\lambda;x) \sim \frac{x^{1-\lambda}}{(1-\lambda)\log x} \qquad \text{as} \quad x\to\infty.$$

The admissible range for λ has been subsequently extended to $0 < \lambda < 1/4$ by Balog [10] and Harman [76], while Harman and Lewis [81] showed that $\mathcal{S}_\lambda$ is infinite for $0 < \lambda < 0.262$.

The first to study the sequence (2.13) was Piatetski-Shapiro [185], who considered $\mathcal{P}_c$ as a sequence of primes represented by a "polynomial of degree c". Piatetski-Shapiro proved that $\mathcal{P}_c$ is infinite when $1 < c < 12/11$. The range for c has been extended several times and it is currently known (see Rivat and Wu [199]) that $\mathcal{P}_c$ is infinite when $1 < c < 243/205$. Furthermore, it is known (see Rivat and Sargos [198]) that when $1 < c < 1.16117\ldots$, we have

$$\pi(\mathcal{P}_c; x) \sim \frac{x^{1/c}}{\log x} \qquad \text{as} \quad x \to \infty.$$

3 The Hardy–Littlewood circle method

Most of the results mentioned in the Introduction have been proved by means of the Hardy–Littlewood circle method. In this section, we describe the general philosophy of the circle method, using its applications to the Goldbach and Waring–Goldbach problems to illustrate the main points.

3.1 Vinogradov's three prime theorem

3.1.1 Preliminaries

Using the orthogonality relation

$$\int_0^1 e(\alpha m)\, d\alpha = \begin{cases} 1, & \text{if } m = 0, \\ 0, & \text{if } m \neq 0, \end{cases} \tag{3.1}$$

we can express $R(n)$ as a Fourier integral. We have

$$\begin{aligned} R(n) &= \sum_{p_1,p_2,p_3 \le n} \int_0^1 e\left(\alpha\left(p_1 + p_2 + p_3 - n\right)\right)\, d\alpha \\ &= \int_0^1 f(\alpha)^3 e(-\alpha n)\, d\alpha, \end{aligned} \tag{3.2}$$

where $f(\alpha)$ is the exponential sum (1.2).

The circle method uses (3.2) to derive an asymptotic formula for $R(n)$ from estimates for $f(\alpha)$. The analysis of the right side of (3.2) rests on the observation that the behavior of $f(\alpha)$ depends on the distance from α to the set of fractions with "small" denominators. When α is "near" such a fraction, we expect $f(\alpha)$ to be "large" and to have certain asymptotic behavior. Otherwise, we can argue that the numbers $e(\alpha p)$ are uniformly distributed on the unit circle and hence $f(\alpha)$ is "small". In order to make these observations rigorous, we need to introduce some notation. Let B be a positive constant to be chosen later and set

$$P = (\log n)^B. \tag{3.3}$$

If a and q are integers with $1 \le a \le q \le P$ and $(a,q)=1$, we define the *major arc*[6]

$$\mathfrak{M}(q,a) = \left[\frac{a}{q} - \frac{P}{qn}\,,\, \frac{a}{q} + \frac{P}{qn}\right]. \tag{3.4}$$

The integration in (3.2) can be taken over any interval of length one and, in particular, over $\big[Pn^{-1}, 1+Pn^{-1}\big]$. We partition this interval into two subsets:

$$\mathfrak{M} = \bigcup_{q\le P} \bigcup_{\substack{1\le a\le q\\(a,q)=1}} \mathfrak{M}(q,a) \quad \text{and} \quad \mathfrak{m} = \big[Pn^{-1}, 1+Pn^{-1}\big] \setminus \mathfrak{M}, \tag{3.5}$$

called respectively the *set of major arcs* and the *set of minor arcs*. Then from (3.2) and (3.5) it follows that

$$R(n) = R(n,\mathfrak{M}) + R(n,\mathfrak{m}), \tag{3.6}$$

where we have denoted

$$R(n,\mathfrak{B}) = \int_{\mathfrak{B}} f(\alpha)^3 e(-\alpha n)\, d\alpha.$$

In the next section we explain how, using Theorem 7 and standard results from elementary number theory, one can obtain an asymptotic formula for $R(n,\mathfrak{M})$ (see (3.13) below). Then in §3.1.3 and §3.1.4 we discuss how one can show that $R(n,\mathfrak{m})$ is of a smaller order of magnitude than the main term in that asymptotic formula (see (3.14)).

3.1.2 The major arcs

In this section we sketch the estimation of the contribution from the major arcs. The interested reader will find the missing details in [116, Chapter 10] or [228, Chapter 2].

It is easy to see that the major arcs $\mathfrak{M}(q,a)$ are mutually disjoint. Thus, using (3.4) and (3.5), we can write

$$R(n,\mathfrak{M}) = \sum_{q\le P} \sum_{\substack{1\le a\le q\\(a,q)=1}} \int_{-P/(qn)}^{P/(qn)} f(a/q+\beta)^3 e\big(-(a/q+\beta)n\big)\, d\beta. \tag{3.7}$$

We now proceed to approximate $f\big(a/q+\beta\big)$ by a simpler expression. To motivate our choice of the approximation, we first consider the case $\beta = 0$. We split the sum $f\big(a/q\big)$ into subsums according to the residue of p modulo q and take into account the definition (2.6). We get

[6]This term may seem a little peculiar at first, given that $\mathfrak{M}(q,a)$ is in fact an interval. The explanation is that, in the original version of the circle method, Hardy and Littlewood used power series and Cauchy's integral formula instead of exponential sums and (3.1) (see [228, §1.2]). In that setting, the role of $\mathfrak{M}(q,a)$ is played by a small circular arc near the root of unity $e(a/q)$.

$$f\left(\frac{a}{q}\right) = \sum_{h=1}^{q} \sum_{\substack{p \le n \\ p \equiv h \pmod q}} e\left(\frac{ap}{q}\right) = \sum_{h=1}^{q} e\left(\frac{ah}{q}\right) \pi(n; q, h).$$

The contribution of the terms with $(h, q) > 1$ is negligible (at most q). If $(h, q) = 1$, our choice (3.3) of the parameter P ensures that we can appeal to Theorem 7 to approximate $\pi(n; q, h)$ by $\phi(q)^{-1} \operatorname{li} n$. We deduce that

$$f\left(\frac{a}{q}\right) = \frac{\operatorname{li} n}{\phi(q)} \sum_{\substack{h=1 \\ (h,q)=1}}^{q} e\left(\frac{ah}{q}\right) + O\left(qnP^{-4}\right). \tag{3.8}$$

The exponential sum on the right side of (3.8) is known as the *Ramanujan sum* and is usually denoted by $c_q(a)$. Its value is known for every pair of integers a and q (see [74, Theorem 271]). In particular, when $(a, q) = 1$ we have $c_q(a) = \mu(q)$, where μ is the Möbius function

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ (-1)^k, & \text{if } n = p_1 \cdots p_k \text{ is the product of } k \text{ distinct primes}, \\ 0, & \text{otherwise.} \end{cases} \tag{3.9}$$

The situation does not change much if instead of $\alpha = a/q$ we consider $\alpha = a/q + \beta \in \mathfrak{M}(q, a)$. In this case we find that

$$f\left(\frac{a}{q} + \beta\right) = \frac{\mu(q)}{\phi(q)} \cdot v(\beta) + O\left(nP^{-3}\right), \tag{3.10}$$

where

$$v(\beta) = \int_2^n \frac{e(\beta u)}{\log u}\, du.$$

Raising (3.10) to the third power and inserting the result into the right side of (3.7), we obtain

$$R(n, \mathfrak{M}) = \sum_{q \le P} \frac{\mu(q) c_q(-n)}{\phi(q)^3} \int_{-P/(qn)}^{P/(qn)} v(\beta)^3 e(-\beta n)\, d\beta + O\left(n^2 P^{-1}\right). \tag{3.11}$$

At this point, we extend the integration over β to the whole real line, and then the summation over q to all positive integers. The arising error terms can be controlled easily by means of well-known bounds for the functions $v(\beta)$ and $\phi(q)$, and we find that

$$R(n, \mathfrak{M}) = \mathfrak{S}(n) J(n) + O\left(n^2 P^{-1}\right), \tag{3.12}$$

where $\mathfrak{S}(n)$ and $J(n)$ are the *singular series* and the *singular integral* defined by

$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} \frac{\mu(q) c_q(-n)}{\phi(q)^3}, \qquad J(n) = \int_{-\infty}^{\infty} v(\beta)^3 e(-\beta n)\, d\beta.$$

The series $\mathfrak{S}(n)$ actually satisfies (1.4). Indeed, the function

$$g(q) = \mu(q)c_q(-n)\phi(q)^{-3}$$

is *multiplicative* in q, that is, $g(q_1q_2) = g(q_1)g(q_2)$ whenever $(q_1, q_2) = 1$. Hence, using the absolute convergence of $\mathfrak{S}(n)$ and the elementary properties of the arithmetic functions involved in the definition of $g(q)$, we can represent the singular series as an Euler product:

$$\begin{aligned}\mathfrak{S}(n) = \sum_{q=1}^{\infty} g(q) &= \prod_{p} \left(1 + g(p) + g(p^2) + \cdots\right) \\ &= \prod_{p|n} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p\nmid n} \left(1 + \frac{1}{(p-1)^3}\right).\end{aligned}$$

Also, an application of Fourier's inversion formula and some calculus reveal that

$$J(n) = \frac{n^2}{2(\log n)^3} + O\left(n^2(\log n)^{-4}\right).$$

Therefore, if $B \geq 4$ we can conclude that

$$R(n, \mathfrak{M}) = \frac{n^2}{2(\log n)^3}\mathfrak{S}(n) + O\left(n^2(\log n)^{-4}\right). \tag{3.13}$$

3.1.3 The minor arcs

In view of (3.6) and (3.13), it suffices to prove that (for some $B \geq 4$)

$$R(n, \mathfrak{m}) \ll n^2(\log n)^{-4}. \tag{3.14}$$

We have

$$|R(n, \mathfrak{m})| \leq \int_{\mathfrak{m}} |f(\alpha)|^3 \, d\alpha \leq \Big(\sup_{\mathfrak{m}} |f(\alpha)|\Big) \int_0^1 |f(\alpha)|^2 \, d\alpha. \tag{3.15}$$

By Parseval's identity and the Prime Number Theorem,

$$\int_0^1 |f(\alpha)|^2 \, d\alpha = \sum_{p \leq n} 1 \ll n(\log n)^{-1}. \tag{3.16}$$

Thus, (3.14) will follow from (3.15), if we show that

$$\sup_{\mathfrak{m}} |f(\alpha)| \ll n(\log n)^{-3}. \tag{3.17}$$

We note that the trivial estimate for $f(\alpha)$ is

$$f(\alpha) \ll \sum_{p \leq n} 1 \ll n(\log n)^{-1},$$

so in order to establish (3.17), we have to save a power of $\log n$ over this trivial estimate (uniformly with respect to $\alpha \in \mathfrak{m}$). We can do this using the following lemma, which provides such a saving under the assumption that α can be approximated by a reduced fraction whose denominator q is "neither too small, nor too large."

Lemma 3.1. *Let α be real and let a and q be integers satisfying*

$$1 \le q \le n, \quad (a,q) = 1, \quad |q\alpha - a| \le q^{-1}.$$

Then

$$f(\alpha) \ll (\log n)^3 \left(nq^{-1/2} + n^{4/5} + n^{1/2}q^{1/2}\right).$$

This is the sharpest known version of the estimate for $f(\alpha)$ established by I. M. Vinogradov [236] in 1937. As we mentioned in the Introduction, that result was the main innovation in Vinogradov's proof of Theorem 1. The above version is due to Vaughan [225].

We shall explain the proof of Lemma 3.1 in the next section and now we shall use it to establish (3.17). To this end we need also the following lemma, known as *Dirichlet's theorem on diophantine approximation*; its proof is elementary and can be found in [228, Lemma 2.1].

Lemma 3.2 (Dirichlet). *Let α and Q be real and $Q \ge 1$. There exist integers a and q such that*

$$1 \le q \le Q, \quad (a,q) = 1, \quad |q\alpha - a| < Q^{-1}.$$

Let $\alpha \in \mathfrak{m}$. By (3.5) and Lemma 3.2 with $Q = nP^{-1}$, there are integers a and q such that

$$P < q \le nP^{-1}, \quad (a,q) = 1, \quad |q\alpha - a| < Pn^{-1} \le q^{-1}.$$

Hence, an appeal to (3.3) and Lemma 3.1 gives

$$f(\alpha) \ll (\log n)^3 \left(nP^{-1/2} + n^{4/5}\right) \ll n(\log n)^{3-B/2}. \tag{3.18}$$

and (3.17) follows on choosing $B \ge 12$. This completes the proof of Theorem 1.

The above proof of Vinogradov's theorem employs the Siegel–Walfisz theorem and, therefore, is ineffective (recall the remark following the statement of Theorem 7). The interested reader can find an effective proof (with a slightly weaker error term) in [116, Chapter 10].

3.1.4 The estimation of $f(\alpha)$

The main tool in the proof of Lemma 3.1 are estimates for bilinear sums of the form

$$S = \sum_{\substack{X < x \le 2X \\ xy \le n}} \sum_{Y < y \le 2Y} \xi_x \eta_y e(\alpha xy). \tag{3.19}$$

We need to control two kinds of such sums, known as *type I sums* and *type II sums*. For simplicity, we describe these two types of sums in the simplest cases, noting that the more general sums arising in the actual proof of Lemma 3.1 can be reduced to these special cases using standard trickery:

- type I sums: sums (3.19) with $|\xi_x| \le 1$, $\eta_y = 1$ for all y, and X is "not too large";
- type II sums: sums (3.19) with $|\xi_x| \le 1$, $|\eta_y| \le 1$, and X, Y are "neither large, nor small".

Vinogradov reduced the estimation of $f(\alpha)$ to the estimation of type I and type II sums by means of an intricate combinatorial argument. Nowadays we can achieve the same result almost instantaneously by referring to the combinatorial identities of Vaughan [223, 225] or Heath-Brown [84]. Let $\Lambda(k)$ denote von Mangoldt's function, whose value is $\log p$ or 0 according as k is a power of a prime p or not. Vaughan's identity states that if U and V are real parameters exceeding 1, then

$$\Lambda(k) = \sum_{\substack{dm=k \\ 1\le d\le V}} \mu(d)\log m - \sum_{\substack{dlm=k \\ 1\le d\le V \\ 1\le m\le U}} \mu(d)\Lambda(m) - \sum_{\substack{dlm=k \\ 1\le d\le V \\ m>U, dl>V}} \mu(d)\Lambda(m). \tag{3.20}$$

Heath-Brown's identity states that if $k \le x$ and J is a positive integer, then

$$\Lambda(k) = \sum_{j=1}^{J} \binom{J}{j} (-1)^{j-1} \sum_{\substack{m_1\cdots m_{2j}=k \\ m_1,\dots,m_j\le x^{1/J}}} \mu(m_1)\cdots\mu(m_j)\log m_{2j},$$

where $\mu(m)$ is the Möbius function.

Both identities can be used to reduce $f(\alpha)$ to type I and type II sums with equal success. Here, we apply Vaughan's identity with $U = V = n^{2/5}$. We obtain

$$\sum_{k\le n} \Lambda(k) e(\alpha k) = W_1 - W_2 - W_3, \tag{3.21}$$

with

$$W_j = \sum_{k\le n} a_j(k) e(\alpha k) \quad (1 \le j \le 3)$$

where $a_j(k)$ denotes the jth sum on the right side of (3.20). The estimation of the sum on the left side of (3.21) is essentially equivalent to that of $f(\alpha)$. The sums W_1 and W_2 on the right side of (3.21) can be reduced to type I sums with $X \ll n^{4/5}$; W_3 can be reduced to type II sums with $n^{2/5} \ll X, Y \ll n^{3/5}$. The reader can find all the details in the proof of [228, Theorem 3.1]. Here we will be content with a brief description of the estimation of the type I and type II sums.

Consider a type I sum S_1. We have

$$|S_1| \le \sum_{X<x\le 2X} \Big| \sum_{Y<y\le Y'} e(\alpha xy)\Big|, \tag{3.22}$$

where $Y' = \min(2Y, n/x)$. We can estimate the inner sum in (3.22) by means of the elementary bound

$$\Big| \sum_{a<y\le b} e(\alpha y)\Big| \le \min\left(b-a+1, \|\alpha\|^{-1}\right), \tag{3.23}$$

where $\|\alpha\|$ denotes the distance from α to the nearest integer. This inequality follows on noting that the sum on the left is the sum of a geometric progression. We obtain

$$|S_1| \le \sum_{x \le 2X} \min\left(Y, \|\alpha x\|^{-1}\right) = T(\alpha), \qquad \text{say.} \tag{3.24}$$

Obviously, the trivial estimate for $T(\alpha)$ is

$$T(\alpha) \ll XY.$$

However, under the hypotheses of Lemma 3.1, one can establish by elementary methods that (see [228, Lemma 2.2])

$$T(\alpha) \ll XY\left(\frac{1}{q} + \frac{1}{Y} + \frac{q}{XY}\right)\log(2XYq). \tag{3.25}$$

Inserting this bound into the right side of (3.24), we obtain a satisfactory bound for S_1.

To estimate a type II sum S_2, we first apply Cauchy's inequality and get

$$|S_2|^2 \ll Y \sum_{Y < y \le 2Y} \Big| \sum_{X < x \le X'} \xi_x e(\alpha xy)\Big|^2,$$

where $X' = \min(2X, n/y)$. Squaring out and interchanging the order of summation, we deduce

$$\begin{aligned} |S_2|^2 &\ll Y \sum_{Y < y \le 2Y} \sum_{X < x_1, x_2 \le X'} \xi_{x_1}\overline{\xi}_{x_2} e(\alpha(x_1 - x_2)y) \\ &\ll Y \sum_{X < x_1, x_2 \le 2X} \Big| \sum_{Y < y \le Y'} e(\alpha(x_1 - x_2)y)\Big| \\ &\ll Y \sum_{X < x \le 2X} \sum_{|h| < X} \Big| \sum_{Y < y \le Y'} e(\alpha hy)\Big|, \end{aligned}$$

where $Y < Y' \le 2Y$. We remark that the innermost sum is now free of "unknown" weights and can be estimated by means of (3.23). We get

$$|S_2|^2 \ll XY^2 + XYT(\alpha), \tag{3.26}$$

and (3.25) again leads to a satisfactory bound for S_2.

3.2 The exceptional set in Goldbach's problem

We now sketch the proof of (1.5). We will not discuss the proof of the more sophisticated results of Montgomery and Vaughan [173] and Pintz [186], since they require knowledge of the properties of Dirichlet L-functions far beyond the scope of this survey. The reader can

find excellent expositions of the Montgomery–Vaughan result in their original paper and also in the monograph [177].

For an even integer n, let $r(n)$ denote the number of representations of n as the sum of two primes, let $\mathcal{Z}(N)$ denote the set of even integers $n \in (N, 2N]$ with $r(n) = 0$, and write $Z(N) = |\mathcal{Z}(N)|$. Since

$$E(x) = \sum_{j=1}^{\infty} Z(x2^{-j}),$$

it suffices to bound $Z(N)$ for large N.

Define $f(\alpha)$, $\mathfrak{M}$, and $\mathfrak{m}$ as before, with N in place of n. When n is an even integer in $(N, 2N]$, a variant of the method in §3.1.2 gives

$$\int_{\mathfrak{M}} f(\alpha)^2 e(-\alpha n)\, d\alpha = \mathfrak{S}_2(n) \frac{n}{(\log n)^2} + O\left(\frac{N}{(\log N)^3}\right),$$

where

$$\mathfrak{S}_2(n) = \prod_{p \nmid n} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \mid n} \left(\frac{p}{p-1}\right)$$

is the singular series. In particular, we have $\mathfrak{S}_2(n) \geq 1$ for even n. Thus, for $n \in \mathcal{Z}(N)$, we have

$$\left| \int_{\mathfrak{m}} f(\alpha)^2 e(-\alpha n)\, d\alpha \right| = \left| - \int_{\mathfrak{M}} f(\alpha)^2 e(-\alpha n)\, d\alpha \right| \gg N(\log N)^{-2}, \tag{3.27}$$

whence

$$Z(N) \ll N^{-2} (\log N)^4 \sum_{n \in \mathcal{Z}(N)} \left| \int_{\mathfrak{m}} f(\alpha)^2 e(-\alpha n)\, d\alpha \right|^2. \tag{3.28}$$

On the other hand, by Bessel's inequality,

$$\sum_{n \in \mathcal{Z}(N)} \left| \int_{\mathfrak{m}} f(\alpha)^2 e(-\alpha n)\, d\alpha \right|^2 \leq \int_{\mathfrak{m}} |f(\alpha)|^4\, d\alpha, \tag{3.29}$$

and (3.16) and (3.18) yield

$$\int_{\mathfrak{m}} |f(\alpha)|^4\, d\alpha \leq \Big(\sup_{\alpha \in \mathfrak{m}} |f(\alpha)| \Big)^2 \int_0^1 |f(\alpha)|^2\, d\alpha \ll N^3 P^{-1} (\log N)^5. \tag{3.30}$$

Combining (3.28)–(3.30), we conclude that

$$Z(N) \ll N P^{-1} (\log N)^9 \ll N (\log N)^{-A},$$

on choosing, say, $P = (\log N)^{A+9}$. This completes the proof of (1.5).

3.3 The circle method in the Waring–Goldbach problem

We now turn our attention to Theorems 3 and 4. Much of the discussion in §3.1 can be generalized to kth powers ($k \geq 2$). Using (3.1), we can write $R^*_{k,s}(n)$ as

$$R^*_{k,s}(n) = \int_0^1 f(\alpha)^s e(-\alpha n)\, d\alpha,$$

where now

$$f(\alpha) = \sum_{p \leq N} e\left(\alpha p^k\right), \quad N = n^{1/k}.$$

Define the sets of major and minor arcs as before (that is, by (3.4) and (3.5), with $P = (\log N)^B$ and $B = B(k,s)$ to be chosen later). The machinery in §3.1.2 generalizes to kth powers with little extra effort. The argument leading to (3.10) gives

$$f\left(\frac{a}{q} + \beta\right) = \phi(q)^{-1} S(q,a)\, v(\beta) + \text{ error term}, \tag{3.31}$$

where $S(q,a)$ is defined by (1.13) and

$$v(\beta) = \int_2^N \frac{e\left(\beta u^k\right)}{\log u}\, du.$$

We now raise (3.31) to the sth power and integrate the resulting approximation for $f(\alpha)^s$ over $\mathfrak{M}$. Using known estimates for $v(\beta)$ and $S(q,a)$, we find that when $s \geq k+1$,

$$\int_{\mathfrak{M}} f(\alpha)^s e(-\alpha n)\, d\alpha = \mathfrak{S}^*_{k,s}(n) J^*_{k,s}(n) + O\left(N^{s-k} P^{-1/k+\varepsilon}\right), \tag{3.32}$$

where $\mathfrak{S}^*_{k,s}(n)$ is defined by (1.13) and $J^*_{k,s}(n)$ is the singular integral

$$\begin{aligned} J^*_{k,s}(n) &= \int_{-\infty}^{\infty} v(\beta)^s e(-\beta n)\, d\beta \\ &= \frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)} \frac{n^{s/k-1}}{(\log n)^s} + O\left(n^{s/k-1} (\log n)^{-s-1}\right). \end{aligned}$$

This reduces the proof of Theorem 3 to the estimate

$$\int_{\mathfrak{m}} f(\alpha)^s e(-\alpha n)\, d\alpha \ll N^{s-k} (\log N)^{-s-1}. \tag{3.33}$$

Notice that when $k = 1$ and $s = 3$, (3.33) turns into (3.14). Thus, it is natural to try to obtain variants of (3.16) and (3.17) for $f(\alpha)$ when $k \geq 2$. To estimate the maximum of $f(\alpha)$ on the minor arcs, we use the same tools as in §3.1.4, that is:

- Heath-Brown's or Vaughan's identity to reduce the estimation of $f(\alpha)$ to the estimation of bilinear sums
$$\sum_{\substack{X<x\le 2X\\ xy\le N}}\sum_{Y<y\le 2Y}\xi_x\eta_y e\left(\alpha(xy)^k\right);$$
- Cauchy's inequality to bound those bilinear sums in terms of the quantity $T(\alpha)$ appearing in (3.24).

The following result due to Harman [75] is the analogue of Lemma 3.1 for $k \ge 2$.

Lemma 3.3. *Let $k \ge 2$, let $\alpha \in \mathbb{R}$, and suppose that a and q are integers satisfying*
$$1 \le q \le N^k, \quad (a,q) = 1, \quad |q\alpha - a| < q^{-1}.$$
There is a constant $c = c(k) > 0$ such that
$$f(\alpha) \ll N(\log N)^c \left(q^{-1} + N^{-1/2} + qN^{-k}\right)^{4^{1-k}}.$$

On choosing the constant B (in the definition of $\mathfrak{m}$) sufficiently large, one can use Lemmas 3.2 and 3.3 to show that, for any fixed $A > 0$,
$$\sup_{\alpha\in\mathfrak{m}} |f(\alpha)| \ll N(\log N)^{-A}.$$
Hence, if $s = 2r+1$, one has
$$\int_{\mathfrak{m}} |f(\alpha)|^s\, d\alpha \le \sup_{\alpha\in\mathfrak{m}} |f(\alpha)| \int_0^1 |f(\alpha)|^{2r}\, d\alpha \ll N(\log N)^{-A}\int_0^1 |f(\alpha)|^{2r}\, d\alpha,$$
and it suffices to establish the estimate
$$I_r(N) := \int_0^1 |f(\alpha)|^{2r} d\alpha \ll N^{2r-k}(\log N)^c, \tag{3.34}$$
with $c = c(k,r)$.

3.4 Mean-value estimates for exponential sums

We now turn to the proof of (3.34). By (3.1), $I_r(N)$ represents the number of solutions of the diophantine equation
$$\begin{cases} x_1^k + \cdots + x_r^k = x_{r+1}^k + \cdots + x_{2r}^k, \\ 1 \le x_1, \dots, x_{2r} \le N \end{cases} \tag{3.35}$$
in *primes* $x_1, \dots, x_{2r}$, and therefore, $I_r(N)$ does not exceed the number of solutions of (3.35) in *integers* $x_1, \dots, x_{2r}$. Using (3.1) to write the latter quantity as a Fourier integral, we conclude that
$$I_r(N) \le \int_0^1 |g(\alpha)|^{2r} d\alpha, \qquad g(\alpha) = \sum_{x\le N} e\left(\alpha x^k\right). \tag{3.36}$$

This reduces the estimation of the even moments of $f(\alpha)$ to the estimation of the respective moments of the exponential sum $g(\alpha)$, whose analysis is much easier. In particular, we have the following two results.

Lemma 3.4 (Hua's lemma). *Suppose that $k \geq 1$, and let $g(\alpha)$ be defined by* (3.36). *There exists a constant $c = c(k) \geq 0$ such that*

$$\int_0^1 |g(\alpha)|^{2^k} d\alpha \ll N^{2^k - k} (\log N)^c. \tag{3.37}$$

Lemma 3.5. *Suppose that $k \geq 11$ and $g(\alpha)$ is defined by* (3.36). *There exists a constant $c = c(k) > 0$ such that for $r > \frac{1}{2}k^2(\log k + \log\log k + c)$,*

$$\int_0^1 |g(\alpha)|^{2r} d\alpha \ll N^{2r-k}. \tag{3.38}$$

These lemmas are, in fact, rather deep and important results in the theory of Waring's problem. Unfortunately, their proofs are too complicated to include in this survey in any meaningful way. The reader will find a proof of a somewhat weaker version of Hua's lemma (with a factor of N^ε in place of $(\log N)^c$) in [228, Lemma 2.5] and a complete proof in [102, Theorem 4]. Results somewhat weaker than Lemma 3.5 are classical and go back to Vinogradov's work on Waring's problem (see [102, Lemma 7.13] or [228, Theorem 7.4]). Lemma 3.5 itself follows from the results in Ford [57] (in particular, see [57, (5.4)]).

Combining (3.36) and Lemmas 3.4 and 3.5, we get (3.34) with

$$r = \begin{cases} 2^{k-1}, & \text{if} \quad k \leq 10, \\ \left[\frac{1}{2}k^2(\log k + \log\log k + c)\right] + 1, & \text{if} \quad k \geq 11. \end{cases}$$

Clearly, this completes the proof of Theorem 3, except for the case $6 \leq k \leq 8$, which we will skip in order to avoid the discussion of certain technical details.

3.5 Diminishing ranges

In this section, we describe the main new idea that leads to the bounds for $H(k)$ in Theorem 4. This idea, known as the *method of diminishing ranges*, appeared for the first time in the work of Hardy and Littlewood on Waring's problem and later was developed into a powerfull technique by Davenport.

The limit of the method employed in §3.3 is set by the mean-value estimates in Lemmas 3.4 and 3.5. The key observation in the method of diminishing ranges is that it can be much easier to count the solutions of the equation in (3.35) if the unknowns $x_1, \ldots, x_{2r}$ are restricted to proper subsets of $[1, N]$. For example, the simplest version of the method that goes back to Hardy and Littlewood uses that when $N_2, \ldots, N_r$ are defined recursively by

$$N_j = k^{-1} N_{j-1}^{1-1/k} \qquad (2 \leq j \leq r),$$

the equation

$$\text{(3.35*)} \qquad \begin{cases} x_1^k + \cdots + x_r^k = x_{r+1}^k + \cdots + x_{2r}^k, \\ N_j < x_j, x_{r+j} \le 2N_j \quad (1 \le j \le r), \end{cases}$$

has only "diagonal" solutions with $x_{r+j} = x_j$, $j = 1, \dots, r$. Thus, the number of solutions of (3.35*) is bounded above by

$$N_1 \cdots N_r \ll N_1^{2-\lambda}(N_2 \cdots N_r)^2$$

where

$$\lambda = 1 + \left(1 - \tfrac{1}{k}\right) + \cdots + \left(1 - \tfrac{1}{k}\right)^{r-1} \ge k - ke^{-r/k}.$$

That is, we have the bound

$$\text{(3.39)} \qquad \int_0^1 \left|g_1(\alpha)g_2(\alpha)\cdots g_r(\alpha)\right|^2 d\alpha \ll N_1^{2-\lambda}(N_2 \cdots N_r)^2,$$

where

$$g_j(\alpha) = \sum_{N_j < x \le 2N_j} e\left(\alpha x^k\right) \quad (1 \le j \le r).$$

We can use (3.39) as a replacement for the mean-value estimates in §3.4. Let $T_{k,s}(n)$ denote the number of solutions of

$$p_1^k + p_2^k + \cdots + p_s^k = n$$

in primes $p_1, \dots, p_s$ subject to

$$N_j < p_j, p_{r+j} \le 2N_j \quad (1 \le j \le r), \qquad N_1 < p_{2r+1}, \dots, p_s \le 2N_1.$$

Then

$$\text{(3.40)} \qquad T_{k,r}(n) = \int_0^1 f_1(\alpha)^{s-2r+2} f_2(\alpha)^2 \cdots f_r(\alpha)^2 e(-\alpha n)\, d\alpha,$$

where

$$f_j(\alpha) = \sum_{N_j < p \le 2N_j} e\left(\alpha p^k\right) \quad (1 \le j \le r).$$

When $r \sim ck \log k$, we can use (3.39) to derive a bound of the form

$$\int_0^1 \left|f_1(\alpha)^2 f_2(\alpha) \cdots f_r(\alpha)\right|^2 d\alpha \ll N_1^{4-k}(N_2 \cdots N_r)^2.$$

Furthermore, assuming that s is just slightly larger than $2r$ (it suffices to assume that $s \ge 2r + 3$, for example), we can then obtain an asymptotic formula for the right side of (3.40) by the methods sketched in §3.3. This is (essentially) how one proves Theorem 4 for $k \ge 11$. The proof for $k \le 10$ follows the same general approach, except that we use more elaborate choices of the parameters $N_1, \dots, N_r$ in (3.35*).

3.6 Kloosterman's refinement of the circle method

Consider again equation (1.9) with $k = 2$. The Hardy–Littlewood method in its original form establishes the asymptotic formula (1.10) for $s > 4$, but it fails to prove Lagrange's four squares theorem. In 1926 Kloosterman [122] proposed a variant of the circle method, known today as *Kloosterman's refinement*, which he used to prove an asymptotic formula for the number of solutions of the equation

$$a_1x_1^2 + \cdots + a_4x_4^2 = n, \tag{3.41}$$

where a_i are fixed positive integers.

Denote by $I(n)$ the number of solutions of (3.41) in positive integers x_i. By (3.1),

$$I(n) = \int_0^1 H(\alpha)e(-\alpha n)\,d\alpha, \tag{3.42}$$

where

$$H(\alpha) = h(a_1\alpha)\cdots h(a_4\alpha), \qquad h(\alpha) = \sum_{x\le N} e\left(\alpha x^2\right), \qquad N = n^{1/2}.$$

A "classical" Hardy–Littlewood decomposition of the right side of (3.42) into integrals over major and minor arcs is of little use here, since we cannot prove that the contribution from the minor arcs is smaller than the expected main term. Kloosterman's idea is to eliminate the minor arcs altogether.

The elimination of the minor arcs requires greater care in the handling of the major arcs. Let X be the integer with $X - 1 < N \le X$. It is clear that the integration in (3.42) can be taken over the interval $\left(X^{-1}, 1 + X^{-1}\right]$, which can be represented as a union of disjoint intervals

$$\left(X^{-1}, 1 + X^{-1}\right] = \bigcup_{q\le N} \bigcup_{\substack{1\le a\le q\\(a,q)=1}} \left(\frac{a}{q} - \frac{1}{qq_1}, \frac{a}{q} + \frac{1}{qq_2}\right], \tag{3.43}$$

where for each pair q, a in the union, the positive integers $q_1 = q_1(q, a)$ and $q_2 = q_2(q, a)$ are uniquely determined and satisfy the conditions

$$N < q_1, q_2 \le 2N, \qquad aq_1 \equiv 1 \pmod q, \qquad aq_2 \equiv -1 \pmod q. \tag{3.44}$$

The decomposition (3.43) is known as the *Farey decomposition* and provides a natural way of partitioning of the unit interval into non-overlapping major arcs (see Hardy and Wright [74, Section 3.8]). Let $\mathfrak{M}(q, a)$ denote the interval in the Farey decomposition "centered" at a/q. We have

$$I(n) = \sum_{q\le N} \sum_{\substack{1\le a\le q\\(a,q)=1}} e\Big(\frac{-an}{q}\Big) \int_{\mathfrak{B}(q,a)} H\Big(\frac{a}{q} + \beta\Big)e(-\beta n)\,d\beta, \tag{3.45}$$

where $\mathfrak{B}(q,a)$ is defined by

$$\mathfrak{B}(q,a) = \{\beta \in \mathbb{R} : a/q + \beta \in \mathfrak{M}(q,a)\}. \tag{3.46}$$

We can find an asymptotic formula for the integrand on the right side of (3.45). The contribution of the main term in that asymptotic formula produces the expected main term in the asymptotic formula for $I(n)$. However, in order to obtain a satisfactory bound for the contribution of the error term, we have to take into account the cancellation among terms corresponding to different Farey fractions a/q with the same denominator. To this end, we want to interchange the order of integration and summation over a in (3.45). Since the endpoints of $\mathfrak{B}(q,a)$ depend on a, the total contribution of the error terms can be expressed as

$$\sum_{q\le N} \int_{-1/(qN)}^{1/(qN)} \Big\{ \sum_{\substack{1\le a\le q\\(a,q)=1}}^{(\beta)} E\left(\frac{a}{q}+\beta\right) e\left(\frac{-an}{q}\right) \Big\} e(-\beta n)\, d\beta, \tag{3.47}$$

where $E(a/q+\beta)$ is the error term in the major arc approximation to $H(a/q+\beta)$ and the superscript in $\sum^{(\beta)}$ indicates that the summation is restricted to those a for which $\mathfrak{B}(q,a) \ni \beta$. Using (3.44) and (3.46), we can transform the latter constraint on a into a condition about the multiplicative inverse of a modulo q, that is, the unique residue class $\bar{a}$ modulo q with $\bar{a}a \equiv 1 \pmod{q}$. Thus, a special kind of exponential sums enter the scene: the *Kloosterman sums*

$$K(q;m,n) = \sum_{\substack{x=1\\(x,q)=1}}^{q} e\Big(\frac{mx+n\bar{x}}{q}\Big).$$

There also other (in fact, more substantial) reasons for the Kloosterman sums to appear, but those are too technical to include here.

The success of Kloosterman's method hinges on the existence of sufficiently sharp estimates for $K(q;m,n)$. The first such estimate was found by Kloosterman himself and later his result has been improved. Today it is known that

$$|K(q;m,n)| \le \tau(q)\, q^{1/2}\, (m,n,q)^{1/2}, \tag{3.48}$$

where (m,n,q) is the greatest common divisor of m,n,q and $\tau(q)$ is the number of positive divisors of q. In 1948 A. Weil [243] proved (3.48) in the most important case: when q is a prime. In the general case (3.48) was established by Estermann [55]. This estimate plays an important role not only in the Kloosterman refinement of the circle method, but in many other problems in number theory.

Kloosterman's method has been applied to several additive problems, and in particular, to problems with primes and almost primes. We refer the reader, for example, to Estermann [56], Hooley [99], Heath-Brown [85, 87, 88], Brüdern and Fouvry [24], Heath-Brown and Tolev [94].

4 Sieve methods

In this section we describe the so-called *sieve methods*, which are an important tool in analytic number theory and, in particular, in the proof of Chen's theorem (Theorem 2 in the Introduction). We start with a brief account of the main idea of the method (§4.1 and §4.2). This allows us in §4.3 to present a proof of a slightly weaker (but much simpler) version of Chen's result, in which P_2-numbers are replaced by P_4-numbers. We conclude the section by sketching some of the new ideas needed to obtain Chen's theorem in its full strength (§4.4) and of some further work on sieve methods (§4.5).

4.1 The sieve of Eratosthenes

Let $\mathcal{A}$ be a finite integer sequence. We will be concerned with the existence of elements of $\mathcal{A}$ that are primes or, more generally, almost primes P_r, with r bounded. In general, sieve methods reduce such a question to counting the elements $a \in \mathcal{A}$ not divisible by small primes p from some suitably chosen set of primes $\mathfrak{P}$. To be more explicit, we consider a set of prime numbers $\mathfrak{P}$ and a real parameter $z \geq 2$ and define the *sifting function*

$$S(\mathcal{A}, \mathfrak{P}, z) = |\{a \in \mathcal{A} : (a, P(z)) = 1\}|, \quad P(z) = \prod_{\substack{p<z \\ p\in\mathfrak{P}}} p, \tag{4.1}$$

where $|\mathcal{A}|$ denotes the number of elements of a sequence $\mathcal{A}$ (not the cardinality of the underlying set). In applications, the set $\mathfrak{P}$ is usually taken to be the set of possible prime divisors of the elements of $\mathcal{A}$, so the sifting function (4.1) counts the elements of $\mathcal{A}$ free of prime divisors $p < z$.

In order to bound $S(\mathcal{A}, \mathfrak{P}, z)$, we recall the following fundamental property of the Möbius function (see [74, Theorem 263]):

$$\sum_{d|k} \mu(d) = \begin{cases} 1, & \text{if} \quad k = 1, \\ 0, & \text{if} \quad k > 1. \end{cases} \tag{4.2}$$

Using this identity, we can express the sifting function in the form

$$S(\mathcal{A}, \mathfrak{P}, z) = \sum_{a\in\mathcal{A}} \sum_{d|(a,P(z))} \mu(d). \tag{4.3}$$

We can now interchange the order of summation to get

$$S(\mathcal{A}, \mathfrak{P}, z) = \sum_{d|P(z)} \mu(d)|\mathcal{A}_d|, \tag{4.4}$$

where

$$\mathcal{A}_d = \{a \in \mathcal{A} : a \equiv 0 \pmod{d}\}.$$

To this end, we suppose that there exist a (large) parameter X and a multiplicative function $\omega(d)$ such that $|\mathcal{A}_d|$ can be approximated by $X\omega(d)/d$. We write $r(X,d)$ for the error term in this approximation, that is,

$$|\mathcal{A}_d| = X\frac{\omega(d)}{d} + r(X,d). \tag{4.5}$$

We expect $r(X,d)$ to be 'small', at least in some average sense over d. Substituting (4.5) into the right side of (4.4), we find that

$$S(\mathcal{A},\mathfrak{P},z) = XV(z) + R(X,z), \tag{4.6}$$

where

$$V(z) = \sum_{d|P(z)} \mu(d)\frac{\omega(d)}{d}, \quad R(X,z) = \sum_{d|P(z)} \mu(d)r(X,d). \tag{4.7}$$

We would like to believe that, under 'ideal circumstances', (4.6) is an asymptotic formula for the sifting function $S(\mathcal{A},\mathfrak{P},z)$, $XV(z)$ being the main term and $R(X,z)$ the error term. However, such expectations turn out to be unrealistic, as we are about to demonstrate.

Let us try to apply (4.6) to bound above the number of primes $\le x$. We choose

$$\mathcal{A} = \{n \in \mathbb{N} : n \le x\}, \quad \mathfrak{P} = \{p : p \text{ is a prime}\}. \tag{4.8}$$

Then

$$|\mathcal{A}_d| = \left[\frac{x}{d}\right] = \frac{x}{d} + r(x,d), \quad |r(x,d)| \le 1,$$

that is, $X = x$ and $\omega(d) = 1$ for all d. Using an elementary property of multiplicative functions (see [74, Theorem 286]), we can write $V(z)$ as

$$V(z) = \prod_{p<z}\left(1 - \frac{\omega(p)}{p}\right). \tag{4.9}$$

When $\omega(p) = 1$, this identity and an asymptotic formula due to Mertens (see [74, Theorem 429]) reveal that the main term in (4.6) is

$$XV(z) = X\prod_{p<z}\left(1 - \frac{1}{p}\right) \sim X\frac{e^{-\gamma}}{\log z} \qquad \text{as} \quad z \to \infty; \tag{4.10}$$

here $\gamma = 0.5772\ldots$ is Euler's constant. Thus, if $\mathcal{A}$ and $\mathfrak{P}$ are as in (4.8) and $z = x^{1/2}$, the projected 'main term' in (4.6) is $\sim 2e^{-\gamma}x(\log x)^{-1}$ as $x \to \infty$, whereas the true size of the sifting function on the left side is

$$S(\mathcal{A},\mathfrak{P},\sqrt{x}) = \pi(x) - \pi(\sqrt{x}) + 1 \sim \frac{x}{\log x} \qquad \text{as} \quad x \to \infty,$$

by the Prime Number Theorem. Since $2e^{-\gamma} = 1.122\ldots$, we conclude that the 'error term' $R(x, \sqrt{x})$ is in this case of the same order of magnitude as the 'main term'.

Identity (4.6) is known as the *sieve of Eratosthenes–Legendre*. The basic idea goes back to the ancient Greeks (usually attributed to Eratosthenes), while the formal exposition above is essentially due to Legendre, who used the above argument to show that

$$\pi(x) \ll \frac{x}{\log\log x}.$$

The sieve of Eratosthenes–Legendre can be extremely powerful in certain situations[7], but in most cases the sum $R(X, z)$ contains 'too many' terms for (4.6) to be of any practical use (e.g., in the above example, $R(X, z)$ contains $2^{\pi(z)}$ terms). Modern sieve methods use various clever approximations to the left side of (4.2) to overcome this problem. In the following sections, we describe one of the variants of one the existing approaches. The reader can find other constructions, comparisons of the various approaches, and proofs in the monographs on sieve methods [63, 66, 174] or in [90] (see also the remarks in §4.5 for other references).

4.2 The linear sieve

Let $y > 0$ be a parameter to be chosen later in terms of X and suppose that $\lambda^+(d)$ and $\lambda^-(d)$ are real-valued functions supported on the squarefree integers d (i.e., $\lambda^\pm(d) = 0$ if d is divisible by the square of a prime). Furthermore, suppose that

$$|\lambda^\pm(d)| \le 1 \quad \text{and} \quad \lambda^\pm(d) = 0 \quad \text{for} \ \ d \ge y, \tag{4.11}$$

and that

$$\sum_{d|n} \lambda^-(d) \le \sum_{d|n} \mu(d) \le \sum_{d|n} \lambda^+(d) \quad \text{for all} \ \ n = 1, 2, \ldots. \tag{4.12}$$

Using (4.3) and the left inequality in (4.12), we obtain

$$S(\mathcal{A}, \mathfrak{P}, z) \ge \sum_{a\in\mathcal{A}} \sum_{d|(a,P(z))} \lambda^-(d).$$

We can interchange the order of summation in the right side of this inequality and apply (4.5) and (4.11) to get the bound

$$\begin{aligned} S(\mathcal{A}, \mathfrak{P}, z) &\ge \sum_{d|P(z)} \lambda^-(d)|\mathcal{A}_d| = \sum_{d|P(z)} \lambda^-(d) \left(X\frac{\omega(d)}{d} + r(X, d) \right) \\ &= X \sum_{d|P(z)} \lambda^-(d)\frac{\omega(d)}{d} + \sum_{d|P(z)} \lambda^-(d) r(X, d) \ge X\mathcal{M}^- - \mathcal{R}, \end{aligned}$$

[7]For example, I. M. Vinogradov's combinatorial argument for converting sums over primes into linear combinations of type I and type II sums is based on a variant of (4.6). See Harman [79] for other applications and further discussion.

where

$$\mathcal{M}^{\pm} = \sum_{d \mid P(z)} \lambda^{\pm}(d) \frac{\omega(d)}{d}, \quad \mathcal{R} = \sum_{\substack{d \mid P(z) \\ d<y}} |r(X,d)|. \tag{4.13}$$

In a similar fashion, we can use the right inequality in (4.12) to estimate the sifting function from above. That is, we have

$$X\mathcal{M}^{-} - \mathcal{R} \le S(\mathcal{A}, \mathfrak{P}, z) \le X\mathcal{M}^{+} + \mathcal{R}. \tag{4.14}$$

We are now in a position to overcome the difficulty caused by the "error term" in the Eratosthenes–Legendre sieve. The sum $\mathcal{R}$ is similar to the error term $R(X,z)$ defined in (4.7), but unlike $R(X,z)$ we can use the parameter y to control the number of terms in $\mathcal{R}$. Thus, our general strategy will be to construct functions $\lambda^{\pm}(d)$ which satisfy (4.11) and (4.12) and for which the sums $\mathcal{M}^{\pm}$ are of the same order as the sum $V(z)$ defined in (4.7). There are various constructions of such functions $\lambda^{\pm}(d)$. However, since it is not our goal to give a detailed treatment of sieve theory here, we will simply state one of the modern sieves in a form suitable for an application to the binary Goldbach problem.

The sieve method we will use is known as the *Rosser–Iwaniec sieve*. Its idea appeared for the first time in an unpublished manuscript by Rosser. The full-fledged version of this sieve was developed independently by Iwaniec [105, 106]. Suppose that the multiplicative function ω in (4.5) satisfies the condition

$$\prod_{w_1 \le p < w_2} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \le \left(\frac{\log w_2}{\log w_1}\right)^{\kappa} \left(1 + \frac{K}{\log w_1}\right) \quad (2 \le w_1 < w_2), \tag{4.15}$$

where $\kappa > 0$ is an absolute constant known as the *sieve dimension* and $K > 0$ is independent of w_1 and w_2. This inequality is usually interpreted as an average bound for the values taken by $\omega(p)$ when p is prime, since it is consistent with the inequality $\omega(p) \le \kappa$. In our application of the sieve to Goldbach's problem, we will have to deal with a sequence $\mathcal{A}$ (given by (1.7)) for which (4.15) holds with $\kappa = 1$, so we will state the Rosser–Iwaniec sieve in this special case, in which it is known as the *linear sieve*.

Suppose that $\omega(p)$ satisfies (4.15) with $\kappa = 1$ and that

$$0 < \omega(p) < p \quad \text{when } p \in \mathfrak{P} \qquad \text{and} \qquad \omega(p) = 0 \quad \text{when } p \notin \mathfrak{P}. \tag{4.16}$$

We put $\lambda^{\pm}(1) = 1$ and $\lambda^{\pm}(d) = 0$ if d is not squarefree. If $d > 1$ is squarefree and has prime decomposition $d = p_1 \cdots p_r$, $p_1 > p_2 > \cdots > p_r$, we define

$$\lambda^{+}(d) = \begin{cases} (-1)^r & \text{if } p_1 \cdots p_{2l} p_{2l+1}^3 < y \text{ whenever } 0 \le l \le (r-1)/2, \\ 0 & \text{otherwise,} \end{cases} \tag{4.17}$$

$$\lambda^{-}(d) = \begin{cases} (-1)^r & \text{if } p_1 \cdots p_{2l-1} p_{2l}^3 < y \text{ whenever } 1 \le l \le r/2, \\ 0 & \text{otherwise.} \end{cases} \tag{4.18}$$

It can be shown (see [63, 105]) that these two functions satisfy conditions (4.11) and (4.12). Furthermore, if the quantities $\mathcal{M}^{\pm}$ are defined by (4.13) with $\lambda^{\pm}(d)$ given by (4.17) and (4.18), we have

$$V(z) \le \mathcal{M}^{+} \le V(z)\big(F(s) + O\big(e^{-s}(\log y)^{-1/3}\big)\big) \qquad \text{for} \quad s \ge 1, \tag{4.19}$$

$$V(z) \ge \mathcal{M}^{-} \ge V(z)\big(f(s) + O\big(e^{-s}(\log y)^{-1/3}\big)\big) \qquad \text{for} \quad s \ge 2, \tag{4.20}$$

where $s = \log y/\log z$ and the functions $f(s)$ and $F(s)$ are the continuous solutions of a system of differential delay equations (see [63, 105]). The analysis of that system reveals that the function $F(s)$ is strictly decreasing for $s > 0$, that the function $f(s)$ is strictly increasing for $s > 2$, and that

$$0 < f(s) < 1 < F(s) \qquad \text{for} \quad s > 2. \tag{4.21}$$

Furthermore, both functions are very close to 1 for large s. More precisely, they satisfy

$$F(s),\ f(s) = 1 + O(s^{-s}) \qquad \text{as} \quad s \to \infty. \tag{4.22}$$

Substituting (4.19) and (4.20) into (4.14), we obtain

$$S(\mathcal{A}, \mathfrak{P}, z) \le XV(z)\big(F(s) + O\big((\log y)^{-1/3}\big)\big) + \mathcal{R} \qquad \text{for} \quad s \ge 1, \tag{4.23}$$

$$S(\mathcal{A}, \mathfrak{P}, z) \ge XV(z)\big(f(s) + O\big((\log y)^{-1/3}\big)\big) - \mathcal{R} \qquad \text{for} \quad s \ge 2, \tag{4.24}$$

where $\mathcal{R}$ is defined by (4.13).

We now return to our initial goal—namely, to prove that the sequence $\mathcal{A}$ contains almost primes. We want to use (4.24) to show that

$$S(\mathcal{A}, \mathfrak{P}, X^{\alpha}) > 0 \tag{4.25}$$

for some fixed $\alpha > 0$. This will imply the existence of an $a \in \mathcal{A}$ all of whose prime divisors exceed X^{α}. If $|a| \ll X^{g}$ for all $a \in \mathcal{A}$, it will then follow that $\mathcal{A}$ contains a P_r-number, where $r \le g/\alpha$. Clearly, since we want to minimize r, we would like to take α as large as possible. On the one hand, in order to derive (4.25) from (4.24), we need to ensure that the main term in (4.24) is positive and that the error term $\mathcal{R}$ is of a smaller order of magnitude than the main term. It is the balancing of these two requirements that determines the optimal choice for z and, ultimately, the quality of our result. In view of (4.21), the positivity of the main term in (4.24) requires choosing y slightly larger than z^2. On the other hand, while in some applications the estimation of $\mathcal{R}$ is easier than in others, it is always the case that it imposes a restriction on how large we can choose y, and hence, how large we can choose z. In the next section, we demonstrate how this general approach works when applied to the binary Goldbach problem.

4.3 The linear sieve in the binary Goldbach problem

In this section, we apply the linear Rosser–Iwaniec sieve to the sequence $\mathcal{A}$ in (1.7) and the set $\mathfrak{P}$ of odd primes that do not divide n, that is,

$$\mathcal{A} = \mathcal{A}(n) = \{n - p : 2 < p < n\} \qquad \text{and} \qquad \mathfrak{P} = \{p : p > 2,\ p \nmid n\}.$$

It is clear that all elements of $\mathcal{A}$ are odd numbers and that at most $\log n$ of them may have a common prime factor with n (for $(n, n-p) > 1$ implies $p \mid n$, and n has at most $\log n$ odd prime factors). Thus, $\mathfrak{P}$ is the set of "typical" prime divisors of elements of $\mathcal{A}$.

Next, we proceed to define the quantity X and the multiplicative function $\omega(d)$ in (4.5). We have

$$|\mathcal{A}_d| = \sum_{\substack{2<p<n \\ p \equiv n \pmod d}} 1 = \pi(n; d, n) - 1, \tag{4.26}$$

so the prime number theorem for arithmetic progressions suggests the choice

$$X = \operatorname{li} n \quad \text{and} \quad \omega(d) = \begin{cases} d/\phi(d) & \text{if } (d, n) = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{4.27}$$

With this choice, the error terms $r(X, d)$ defined by (4.5) satisfy the inequality

$$|r(X, d)| \le \begin{cases} 1 + \left|\pi(n; d, n) - \dfrac{\operatorname{li} n}{\phi(d)}\right| & \text{if } (d, n) = 1, \\ 1 & \text{otherwise.} \end{cases}$$

It then follows from the Bombieri–Vinogradov theorem (Theorem 8) that

$$\mathcal{R} \le y + \sum_{d \le y} \max_{(a,d)=1} \left|\pi(n; d, a) - \frac{\operatorname{li} n}{\phi(d)}\right| \ll n(\log n)^{-3}, \tag{4.28}$$

whenever $y \le n^{1/2}(\log n)^{-6}$. Furthermore, we have

$$V(z) = \prod_{\substack{p<z \\ p \nmid n}} \left(1 - \frac{1}{p-1}\right) \ge \prod_{p<z} \left(1 - \frac{1}{p-1}\right) \gg (\log z)^{-1}. \tag{4.29}$$

On choosing $y = n^{1/2}(\log n)^{-6}$ and $z = n^{2/9}$, we have

$$\frac{\log y}{\log z} = \frac{9}{4} + O\left(\frac{\log\log n}{\log n}\right) > 2.2,$$

provided that n is sufficiently large. Hence, we deduce from (4.21), (4.24) and (4.27)–(4.29) that

$$S(\mathcal{A}, \mathfrak{P}, z) \gg n(\log n)^{-2}. \tag{4.30}$$

That is, there are $\gg n(\log n)^{-2}$ elements of $\mathcal{A}$ that have no prime divisors smaller than $n^{2/9}$. Since the numbers in $\mathcal{A}$ do not exceed n, the elements of $\mathcal{A}$ counted on the left side of (4.30) have at most four prime divisors each, that is, the left side of (4.30) counts solutions of $n - p = P_4$.

We have some freedom in our choice of parameters in the above argument. For example, we could have set $z = n^\alpha$, where α is any fixed real number in the range $1/5 < \alpha < 1/4$. Of course, what we would really like to do is set $z = n^\alpha$, where $\alpha > 1/4$. With such a choice for z, the above argument would establish the existence of infinitely many solutions to $n - p = P_3$. Unfortunately, our choice of z is restricted (via the condition $s = \log y/\log z > 2$) by the largest value of Q admissible in the Bombieri–Vinogradov theorem. In particular, in order to be able to choose $z = n^{1/4}$, we would need a version of the Bombieri–Vinogradov theorem that holds for $Q \le x^{1/2+\varepsilon}$.

4.4 Weighted sieves and Chen's theorem

The idea of a *weighted sieve* was introduced by Kuhn [124] who observed that instead of the sifting function $S(\mathcal{A}, \mathfrak{P}, z)$ one may consider a more general sum of the type

$$W(\mathcal{A}, \mathfrak{P}, z) = \sum_{\substack{a\in\mathcal{A},\\ (a,P(z))=1}} w(a), \tag{4.31}$$

where $w(a)$ are weights at one's disposal to choose. It is common to use weights of the form

$$w(a) = 1 - \sum_{\substack{p\mid a\\ z\le p<z_1}} \omega_p, \tag{4.32}$$

with suitably chosen $0 \le \omega_p < 1$. With such a choice of $w(a)$, (4.31) can be written in the form

$$W(\mathcal{A}, \mathfrak{P}, z) = S(\mathcal{A}, \mathfrak{P}, z) - \sum_{z\le p<z_1} \omega_p S(\mathcal{A}_p, \mathfrak{P}, p). \tag{4.33}$$

We can now use an ordinary sieve to estimate the right side of (4.33). For example, we can appeal to (4.24) to bound $S(\mathcal{A}, \mathfrak{P}, z)$ from below and to (4.23) to bound each sifting function $S(\mathcal{A}_p, \mathfrak{P}, p)$ from above. If the resulting lower bound for the right side of (4.33) is positive, we then conclude that there exist elements a of $\mathcal{A}$ with $w(a) > 0$. Such numbers a have no prime divisors $p < z$ and the number of their prime divisors with $z \le p < z_1$ can be controlled via the choice of the ω_p's.

The above idea plays an important role in improvements on the result established in §4.3. Using weighted sieves, Buchstab [29] and Richert [196] proved that every sufficiently large even n can be represented as the sum of a prime and a P_3-number. Richert used weights of the form

$$w(a) = 1 - \theta \sum_{\substack{p\mid a\\ z\le p<z_1}} \left(1 - \frac{\log p}{\log z_1}\right),$$

while Buchstab's weights were somewhat more complicated. Chen's proof of Theorem 2 uses weights of the form (4.32) with $z = n^{1/10}$, $z_1 = n^{1/3}$, and

$$\omega_p = \frac{1}{2} + \frac{1}{2}\delta_p(a),$$

where

$$\delta_p(a) = \begin{cases} 1 & \text{if } \ a = pp_1p_2 \ \text{ with } \ p_1 \geq z_1, \\ 0 & \text{otherwise.} \end{cases}$$

Here, n is the even number appearing in the statement of Theorem 2 and a is an element of the sequence (1.7). With this choice of ω_p, successful sifting produces numbers $a \in \mathcal{A}$ with $w(a) > 0$ and no prime divisors $p < n^{1/10}$. One can prove that any such number a must in fact be a P_2-number. The reader can find a detailed proof of Chen's theorem in [66, Chapter 11], [175, Chapter 10], or [178, Chapter 9].

4.5 Other sieve methods

We conclude our discussion of sieve methods with a brief account of some of the important ideas in sieve theory left out of the previous sections.

Selberg's sieve. The Rosser–Iwaniec sieve defined by (4.17) and (4.18) is not particularly sensitive to the arithmetical nature of the sequence $\mathcal{A}$ that is being sifted. In fact, the only piece of information about $\mathcal{A}$ that the Rosser–Iwaniec sieve does take into account is its sieve dimension. Such sieves are known as *combinatorial*. Selberg [204] proposed another approach, which uses the multiplicative function $\omega(d)$ appearing in (4.5) to construct essentially best possible upper sieve weights $\lambda^+(d)$ for a given sequence $\mathcal{A}$.

Suppose that $\rho(d)$ is a real function such that $\rho(1) = 1$. Then

$$\sum_{d|n} \mu(d) \leq \left(\sum_{d|n} \rho(d) \right)^2.$$

We can apply this inequality to estimate $S(\mathcal{A}, \mathfrak{P}, z)$ as follows:

$$\begin{aligned} S(\mathcal{A}, \mathfrak{P}, z) &\leq \sum_{a \in \mathcal{A}} \left(\sum_{d|n} \rho(d) \right)^2 = \sum_{a \in \mathcal{A}} \sum_{d_1, d_2 | n} \rho(d_1)\rho(d_2) \\ &= \sum_{d_1, d_2} \rho(d_1)\rho(d_2) \big| \mathcal{A}_{[d_1, d_2]} \big|, \end{aligned}$$

where $|\mathcal{A}_d|$ is as before and $[d_1, d_2]$ is the least common multiple of d_1 and d_2. Using (4.5), we find that

$$S(\mathcal{A}, \mathfrak{P}, z) \leq XW + \mathcal{R}',$$

where

$$W = \sum_{d_1,d_2} \rho(d_1)\rho(d_2)\frac{\omega([d_1,d_2])}{[d_1,d_2]}, \qquad \mathcal{R}' = \sum_{d_1,d_2} \rho(d_1)\rho(d_2)r(X,[d_1,d_2]).$$

In order to control the "error term" $\mathcal{R}'$, we further assume that $\rho(d) = 0$ when $d > \xi$, where $\xi > 0$ is a parameter. The double sum W is a quadratic form in the variables $\rho(d)$, $1 < d \le \xi$. Selberg's idea is to choose the values of these variables as to minimize this quadratic form.

More information about Selberg's sieve—including the techniques used to construct the lower sieve function $\lambda^-(d)$ of Selberg's sieve—can be found in [66, 174] and in Selberg's collected works [205, 206].

The large sieve. The method known as the *large sieve* was introduced in 1941 by Linnik [140], but its systematic study did not commence until Rényi's work [195] on the binary Goldbach problem. The original idea of Linnik and Rényi evolved into a general analytic principle that has penetrated analytic number theory on many levels (and perhaps does not warrant the name "sieve" anymore, but the term has survived for historical reasons). The most prominent application of the large sieve is the Bombieri–Vinogradov theorem. The reader will find discussion of the number-theoretic aspects of the large sieve in [20, 49, 171] and of the analytic side of the story in [49, 171, 172].

Alternative form of the error term in the sieve. Iwaniec [106] obtained a variant of the linear sieve featuring an error term that is better suited for certain applications than the error term $\mathcal{R}$ defined in (4.13). It is of the form

$$\sum_{\substack{m<M \\ m|P(z)}} \sum_{\substack{n<N \\ n|P(z)}} a_m b_n r(X, mn), \tag{4.34}$$

where the coefficients a_m and b_n are bounded above in absolute value and $r(X, mn)$ are the remainder terms defined earlier. In some applications, one can use the bilinearity of this expression to estimate the double sum when the product MN is larger than the largest value of y for which one can obtain a satisfactory bound for $\mathcal{R}$. Iwaniec [104] used this idea in his proof that certain quadratic polynomials take on infinitely P_2-numbers (recall §2.4).

Prime detecting sieves. For a long time it was believed that sieve methods are not capable of detecting prime numbers; there are even a couple of prominent papers (see [21, 205]) that quantify the shortcomings of the classical sieve technology. In short, classical sieves are incapable of distinguishing between integers having even number of prime divisors and those having an odd number of prime divisors (this is known in sieve theory as the *parity obstacle*). A prime detecting sieve overcomes the parity obstacle by combining the general sieve philosophy with additional analytic information. A variant of the basic idea can be traced all the way back to Vinogradov's work on sums over primes, but the first explicit uses of prime detecting sieves appeared in the late 1970s in investigations of the distribution of primes in short intervals (see [91, 107]). The method flourished during the last decade

and has been instrumental in the proofs of several of the restults mentioned in the previous sections: the result of Friedlander and Iwaniec [58] on prime values of $x^2 + y^4$; the results of Heath-Brown and Moroz [89, 92] on prime values of binary cubic forms; and the result of Baker, Harman, and Pintz [9] on primes in short intervals are just three such examples. Compared to classical sieve methods, the theory of prime detecting sieves is still in its infancy and thus the general literature on the subject is relatively scarce, but the reader eager to learn more about such matters will find two excellent expositions in [59] and [79].

5 Other work on the Waring–Goldbach problem

In the Introduction, we mentioned the cornerstones in the study of the Goldbach and Waring–Goldbach problems. However, as is often the case in mathematics, those results are intertwined with a myriad of other results on various aspects and variants of the two main problems. In this final section, we describe some of the more important results of the latter kind. The circle method, sieve methods, or a combination of them play an essential role in the proofs of all these.

5.1 Estimates for exceptional sets

Inspired by the work of Chudakov [42] and Estermann [54] on the exceptional set in the binary Goldbach problem, Hua studied the function $h(k)$, defined to be the least s such that almost all integers $n \le x$, $n \equiv s \pmod{K(k)}$, can be written as the sum of s kth powers of primes ($K(k)$ is defined by (1.12)). Let $E_{k,s}(x)$ denote the number of exceptions, that is, the number of integers n, with $n \le x$ and $n \equiv s \pmod{K(k)}$, for which (1.14) has no solution in primes $p_1, \dots, p_s$. Hua showed (essentially) that if $H(k) \le s_0(k)$, then $E_{k,s}(x) = o(x)$ for any $s \ge \frac{1}{2}s_0(k)$. Later, Schwarz [202] refined Hua's method to show that

$$E_{k,s}(x) \ll x(\log x)^{-A} \tag{5.1}$$

for any fixed $A > 0$.

In recent years, motivated by the estimate (1.6) of Montgomery and Vaughan, several authors have pursued similar estimates for exceptional sets for squares and higher powers of primes. The first to obtain such an estimate were Leung and Liu [134], who showed that $E_{2,3}(x) \ll x^{1-\delta}$, with an absolute constant $\delta > 0$. Explicit versions of this result were later given in [16, 80, 128, 159, 160], the best result to date being the estimate (see Harman and Kumchev [80])

$$E_{2,3}(x) \ll x^{6/7+\varepsilon}.$$

Furthermore, several authors [80, 147, 149, 155, 249] obtained improvements on Hua's bound (5.1) for $E_{2,4}(x)$, the most recent being the bound

$$E_{2,4}(x) \ll x^{5/14+\varepsilon},$$

established by Harman and Kumchev [80]. Ren [194] studied the exceptional set for sums of five cubes of primes and proved that

$$E_{3,s}(x) \ll x^{1-(s-4)/153} \qquad (5 \le s \le 8).$$

This estimate has since been improved by Wooley [248] and Kumchev [126]. In particular, Kumchev [126] showed that

$$E_{3,5}(x) \ll x^{79/84}, \qquad E_{3,6}(x) \ll x^{31/35},$$
$$E_{3,7}(x) \ll x^{51/84}, \qquad E_{3,8}(x) \ll x^{23/84}.$$

Finally, Kumchev [126] has developed the necessary machinery to obtain estimates of the form $E_{k,s}(x) \ll x^{1-\delta}$, with explicit values of $\delta = \delta(k,s) > 0$, for all pairs of integers $k \ge 4$ and s for which an estimate of the form (5.1) is known.

In 1973 Ramachandra [192] considered the exceptional set for the binary Goldbach problem in short intervals. He proved that if $y \ge x^{7/12+\varepsilon}$ and $A > 0$, then

$$E(x+y) - E(x) \ll y(\log x)^{-A},$$

where the implied constant depends only on A and ε. After a series of improvements on this result [8, 52, 53, 111, 112, 115, 135, 167, 182], this estimate is now known for $y \ge x^{7/108+\varepsilon}$ (see Jia [115]). Lou and Yao [164, 250] were the first to pursue a short interval version of the estimate (1.6) of Montgomery and Vaughan. Their result was substantially improved by Peneva [180] and the best result in this direction, due to Languasco [131], states that there exists a small constant $\delta > 0$ such that

$$E(x+y) - E(x) \ll y^{1-\delta/600},$$

whenever $y \ge x^{7/24+7\delta}$.

Furthermore, J. Liu and Zhan [157] and Mikawa [169] studied the quantity $E_{2,3}(x)$ in short intervals and the latter author showed that

$$E_{2,3}(x+y) - E_{2,3}(x) \ll y(\log x)^{-A}$$

for any fixed $A > 0$ and any $y \ge x^{1/2+\varepsilon}$.

5.2 The Waring–Goldbach problem with almost primes

There have also been attempts to gain further knowledge about the Waring–Goldbach problem by studying closely related but more accessible problems. The most common such variants relax the multiplicative constraint on (some of) the variables. Consider, for example, Lagrange's equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n. \tag{5.2}$$

Greaves [62] proved that every sufficiently large $n \not\equiv 0, 1, 5 \pmod 8$ can be represented in the form (5.2) with x_1, x_2 primes and x_3, x_4 (unrestricted) integers. Later, Plaksin [189] and Shields [207] found independently an asymptotic formula for the number of such representations. Brüdern and Fouvry [24] proved that every sufficiently large integer $n \equiv 4 \pmod{24}$ can be written as the sum of four squares of P_{34}-numbers. Heath-Brown and Tolev [94] established, under the same hypothesis on n, that one can solve (5.2) in one prime and three almost primes of type P_{101} or in four almost primes, each of type P_{25}. Tolev [218] has recently improved the results in [94], replacing the types of the almost primes involved by P_{80} and P_{21}, respectively. We must also mention the recent result by Blomer and Brüdern [17] that all sufficiently large integers n such that $n \equiv 3 \pmod{24}$ and $5 \nmid n$ are sums of three almost primes of type P_{521} (and of type P_{371} if n is also squarefree).

In 1951 Roth [200] proved that if n is sufficiently large, the equation

$$x^3 + p_1^3 + \cdots + p_7^3 = n \tag{5.3}$$

has solutions in primes $p_1, \ldots, p_7$ and an integer x. Brüdern [22] showed that if $n \equiv 4 \pmod{18}$, then x can be taken to be a P_4-number, and Kawada [118] used an idea from Chen's proof of Theorem 2 to obtain a variant of Brüdern's result for almost primes of type P_3. Furthemore, Brüdern [23] proved that every sufficiently large integer is the sum of the cubes of a prime and six almost-primes (five P_5-numbers and a P_{69}-number) and Kawada [119] has shown that every sufficiently large integer is the sum of seven cubes of P_4-numbers.

Wooley [249] showed that all but $O\big((\log x)^{6+\varepsilon}\big)$ integers $n \le x$, satisfying certain natural congruence conditions can be represented in the form (5.2) with prime variables x_1, x_2, x_3 and an integer x_4. Tolev [219] established a result of similar strength for the exceptional set for equation (5.2) with primes x_1, x_2, x_3 and an almost prime x_4 of type P_{11}.

5.3 The Waring–Goldbach problem with restricted variables

Through the years, a number of authors have studied variants of the Goldbach and Waring–Goldbach problems with additional restrictions on the variables. In 1951 Haselgrove [82] announced that every sufficiently large odd integer n is the sum of three primes p_1, p_2, p_3 such that $|p_i - n/3| \le n^{63/64+\varepsilon}$. In other words, one can take the primes in Vinogradov's three prime theorem to be "almost equal". Subsequent work by several mathematicians [7, 34, 109, 110, 177, 254] tightened the range for the p_i's to $|p_i - n/3| \le n^{4/7}$ (see Baker and Harman [7]).

Furthermore, Bauer, Liu, and Zhan [13, 156, 158] considered the problem of representations of an integer as sums of five squares of almost equal primes. The best result to date is due to Liu and Zhan [158], who proved that every sufficiently large integer $n \equiv 5 \pmod{24}$ can be written as

$$n = p_1^2 + \cdots + p_5^2,$$

with primes $p_1, \ldots, p_5$ satisfying $|p_i^2 - n/5| < n^{45/46+\varepsilon}$. Liu and Zhan [156] also showed that the exponent $\frac{45}{46}$ can be replaced by $\frac{19}{20}$ on the assumption of GRH.

In 1986 Wirsing [244] proved that there exist sparse sequences of primes $\mathcal{S}$ such that every sufficiently large odd integer can be represented as the sum of three primes from $\mathcal{S}$. However, his method was probabilistic and did not yield an example of such a sequence. Thus, Wirsing proposed the problem of finding "natural" examples of arithmetic sequences having this property. The first explicit example was given by Balog and Friedlander [12]. They proved that the sequence of Piatetski-Shapiro primes (recall (2.13)) is admissible for $1 < c < 21/20$. Jia [113] improved the range for c to $1 < c < 16/15$, and Peneva [181] studied the binary problem with a Piatetski-Shapiro prime and an almost prime. Tolev [215]–[217] and Peneva [179] considered additive problems with prime variables p such that the integers $p + 2$ are almost-primes. For example, Tolev [217] proved that every sufficiently large $n \equiv 3 \pmod 6$ can be represented as the sum of primes p_1, p_2, p_3 such that $p_1 + 2 = P_2$, $p_1 + 2 = P_5$, and $p_1 + 2 = P_7$. Green and Tao announced at the end of [64] that, using their method, one can prove that there are arbitrarily long non trivial arithmetic progressions consisting of primes p such that $p + 2 = P_2$. They presented in [65] a proof of this result for progressions of three primes.

5.4 Linnik's problem and variants

In the early 1950s Linnik proposed the problem of finding sparse sequences $\mathcal{A}$ such that all sufficiently large integers n (possibly subject to some parity condition) can be represented as sums of two primes and an element of $\mathcal{A}$. He considered two special sequences. First, he showed [143] that if GRH holds, then every sufficiently large odd n is the sum of three primes p_1, p_2, p_3 with $p_1 \ll (\log n)^3$. Montgomery and Vaughan [173] sharpened the bound on p_1 to $p_1 \ll (\log n)^2$ and also obtained an unconditional result with $p_1 \ll n^{7/72+\varepsilon}$; the latter bound has been subsequently improved to $p_1 \ll n^{0.02625}$ (this follows by the original argument of Montgomery and Vaughan from recent results of Baker, Harman, and Pintz [9] and Jia [114]).

Linnik [142, 144] was also the first to study additive representations as sums of two primes and a fixed number of powers of 2. He proved, first under GRH and later unconditionally, that there is an absolute constant r such that every sufficiently large even integer n can be expressed as the sum of two primes and r powers of 2, that is, the equation

$$p_1 + p_2 + 2^{\nu_1} + \cdots + 2^{\nu_r} = n,$$

has solutions in primes p_1, p_2 and non-negative integers $\nu_1, \ldots, \nu_r$. Later Gallagher [60] established the same result by a different method. Several authors have used Gallagher's approach to find explicit values of the constant r above (see [137, 138, 150, 151, 152, 242]); in particular, Li [138] proved that $r = 1906$ is admissible and Wang [242] obtained $r = 160$ under GRH. Recently, Heath-Brown and Puchta [93] and Pintz and Ruzsa [187] made (independently) an important discovery that leads to a substantial improvement on the earlier results. Their device establishes Linnik's result with $r = 13$ (see [93]) and with $r = 7$ under GRH (see [93, 187]). Furthermore, Pintz and Rusza [188] have announced an unconditional proof of the case $r = 8$.

There is a similar approximation to the Waring–Goldbach problem for four squares of primes. J. Y. Liu, M. C. Liu, and Zhan [153, 154] proved that there exists a constant r such that every sufficiently large even integer n can be expressed in the form

$$p_1^2 + p_2^2 + p_3^2 + p_4^2 + 2^{\nu_1} + \cdots + 2^{\nu_r} = n,$$

where $p_1, \ldots, p_4$ are primes and $\nu_1, \ldots, \nu_r$ are non-negative integers. J. Y. Liu and M. C. Liu [148] established this result with $r = 8330$ and considered also the related problem about representations of integers as sums of a prime, two squares of primes and several powers of 2.

5.5 Additive problems with mixed powers

In 1923 Hardy and Littlewood [71] used the general philosophy underlying the circle method to formulate several interesting conjectures. For example, they stated a conjectural asymptotic formula for the number of representations of a large integer n in the form

$$p + x^2 + y^2 = n, \tag{5.4}$$

where p is a prime and x, y are integers. Their prediction was confirmed in the late 1950s, first by Hooley [97] under the assumption of GRH and then unconditionally by Linnik [145]. The reader will find the details of the proof in [98, 146].

In another conjecture, Hardy and Littlewood proposed an asymptotic formula for the number of representations of a large integer n as the sum of a prime and a square. While such a result appears to lie beyond the reach of present methods, Miech [166] showed that this conjecture holds for almost all integers $n \le x$. Let $E_k(x)$, $k \ge 2$, denote the number of integers $n \le x$ such that the equation $n = p + x^k$ has no solution in a prime p and an integer x. Miech obtained the bound $E_2(x) \ll x(\log x)^{-A}$ for any fixed $A > 0$. Subsequent work of Brüdern, Brünner, Languasco, Mikawa, Perelli, Pintz, Polyakov, A. I. Vinogradov, and Zaccagnini [26, 28, 132, 168, 183, 190, 235, 251] extended and sharpened Miech's estimate considerably. Here is a list of some of their results:

- For any fixed $k \ge 2$, we have $E_k(x) \ll x^{1-\delta_k}$, where $\delta_k > 0$ depends at most on k; see [28, 190, 235] for the case $k = 2$ and [183, 251] for the general case.
- Assuming GRH, we have $E_k(x) \ll x^{1-\delta_k}$, where $\delta_k = 1/(k2^k)$ or $\delta_k = 1/(25k)$ according as $2 \le k \le 4$ or $k \ge 5$; see [183] and [26].
- If $k \ge 2$ is a fixed integer and $K = 2^{k-2}$ then there exists a small absolute constant $\delta > 0$ such that
$$E_k(x + y) - E_k(x) \ll y^{1-\delta/(5K)},$$
provided that $x^{(7/12)(1-1/k)+\delta} \le y \le x$; see [132].

Furthermore, several mathematicians [14, 15, 26, 157] obtained variants of the above bounds in the case when the variable x is also restricted to primes, while Zaccagnini [252] studied the more general problem of representing a large integer n in the form $n = p + f(x)$, where $f(X) \in \mathbb{Z}[X]$.

Several interesting theorems were proved by Brüdern and Kawada [25]. For example, one of them states that if k is an integer with $3 \le k \le 5$, then all sufficiently large integers n can be represented as

$$x + p_1^2 + p_2^3 + p_3^k = n,$$

where p_i are primes and $x = P_2$.

5.6 The Waring–Goldbach problem "with coefficients"

In this section we discuss the solubility of equations of the form (1.16), which we introduced in §1.4 as a natural generalization of the Waring–Goldbach problem. There are two substantially different contexts in which one can study this problem. Suppose first that all $a_1, \dots, a_s, n$ are all of the same sign. Then one expects that (1.16) must have solutions for sufficiently large $|n|$. When "sufficiently large" is understood as $|n| \ge C(a_1, \dots, a_s)$, with some unspecified constant depending on the a_j's, this is a trivial modification of the Waring–Goldbach problem (that can be handled using essentially the same tools). On the other hand, the problem of finding solution when $|n|$ is not too large compared to $|\mathbf{a}|_\infty = \max\{|a_1|, \dots, |a_s|\}$ is significantly more challanging. Similarly, if $a_1, \dots, a_s$ are not all of the same sign, one wants to find solutions of (1.16) in primes $p_1, \dots, p_s$ that are not too large compared to $|\mathbf{a}|_\infty$ and $|n|$. Such questions were investigated first by Baker [5], who studied the case $k = 1$ and $s = 3$. Later, Liu and Tsang [161] showed, again for $k = 1$ and $s = 3$, that (1.16) has solutions when:

- a_1, a_2, a_3 are of the same sign and $|n| \gg |\mathbf{a}|_\infty^A$ for some absolute constant $A > 0$;
- a_1, a_2, a_3 are not of the same sign and $\max\{p_1, p_2, p_3\} \ll |\mathbf{a}|_\infty^{A-1} + |n|$.

In these results, the coefficients a_1, a_2, a_3, n must satisfy also certain necessary congruence conditions (which generalize the requirement that n be odd in Vinogradov's three primes theorem). Through the efforts of several mathematicians, the constant A has been evaluated and it is known that the value $A = 38$ is admissible (see Li [139]). Furthermore, if we replace the natural arithmetic conditions on the coefficients by another set of conditions, which are somewhat more restrictive but also simplify greatly the analysis, we can decrease the value of A further. In particular, Choi and Kumchev [38] have shown that $A = 23/3$ is admissible under such stronger hypotheses.

Liu and Tsang [162] studied also the quadratic case of (1.16) in five variables and obtained results similar to those stated above for the linear case. In this problem, explicit values of the analogue of A above were given by Choi and Liu [39, 40], Choi and Kumchev [37], and Harman and Kumchev [80]. In particular, it is proved in [80] that (1.16) with $k = 2$ and $s = 5$ has solutions when:

- $a_1, \dots, a_5$ are of the same sign and $|n| \gg |\mathbf{a}|_\infty^{15+\varepsilon}$;
- $a_1, \dots, a_5$ are not of the same sign and $\max\{p_1, \dots, p_5\} \ll |\mathbf{a}|_\infty^{7+\varepsilon} + |n|^{1/2}$.

5.7 Diophantine inequalities with primes

Some variants of the Waring–Goldbach problem are stated most naturally in terms of diophantine inequalities. The best-known problem of this kind concerns the distribution of the values of the forms

$$\lambda_1 p_1^k + \cdots + \lambda_s p_s^k, \tag{5.5}$$

where k and s are positive integers, $\lambda_1, \dots, \lambda_s$ are nonzero real numbers, and $p_1, \dots, p_s$ are prime variables. It is natural to conjecture that if $\lambda_1, \dots, \lambda_s$ are not all of the same sign and if λ_i/λ_j is irrational for some pair of indices i, j, then the values attained by the form (5.5) are dense in $\mathbb{R}$ whenever $s \ge s_0(k)$. In other words, given any $\varepsilon > 0$ and $\alpha \in \mathbb{R}$, the inequality

$$\left|\lambda_1 p_1^k + \cdots + \lambda_s p_s^k - \alpha\right| < \varepsilon \tag{5.6}$$

should have a solution in primes $p_1, \dots, p_s$. The first results in this problem were obtained by Schwarz [203], who established the solvability of (5.6) under the same restrictions on s as in Theorem 3. Baker [5] and Vaughan [221, 222, 224] proposed the more difficult problem of replacing the fixed number ε on the right side of (5.6) by an explicit function of $\max\{p_1, \dots, p_s\}$ that approaches 0 as $\max\{p_1, \dots, p_s\} \to \infty$. Further work has focused primarily on the case of small k. For example, Harman [78] has shown that under the above assumptions on $\lambda_1, \lambda_2, \lambda_3$, the diophantine inequality

$$\left|\lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3 - \alpha\right| < \max\{p_1, p_2, p_3\}^{-1/5+\varepsilon}$$

has infinitely many solutions in primes p_1, p_2, p_3. Baker and Harman [6] showed that on GRH the exponent $\frac{1}{5}$ in this result can be replaced by $\frac{1}{4}$. Furthermore, Harman [77] proved that if λ_1/λ_2 is a negative irrational number, then for any real α the inequality

$$\left|\lambda_1 p + \lambda_2 P_3 - \alpha\right| < p^{-1/300}$$

has infinitely many solutions in a prime p and a P_3-almost prime. (This improves on an earlier result of Vaughan [224], where the almost prime is a P_4-number.)

In 1952 Piatetski-Shapiro [184] considered a variant of the Waring–Goldbach problem for non-integer exponents $c > 1$. He showed that for any fixed $c > 1$, which is not an integer, there exists an integer $H(c)$ with the following property: if $s \ge H(c)$, the inequality

$$\left|p_1^c + \cdots + p_s^c - \alpha\right| < \varepsilon \tag{5.7}$$

has solutions in primes $p_1, \dots, p_s$ for any fixed $\varepsilon > 0$ and $\alpha \ge \alpha_0(\varepsilon, c)$. In particular, Piatetski-Shapiro showed that $H(c) \le 5$ for $1 < c < 3/2$. Motivated by Vinogradov's three

prime theorem, Tolev [213] proved that $H(c) \leq 3$ for $1 < c < 15/14$. The range of validity of Tolev's result was subsequently extended by several authors [32, 33, 125, 130]; in particular, Kumchev [125] has given the range $1 < c < 61/55$. Furthemore, it follows from the work of Kumchev and Laporta [129, 133] that $H(c) \leq 4$ for $1 < c < 6/5$ and for almost all (in the sense of Lebesgue measure) $1 < c < 2$, while Garaev [61] has showed that $H(c) \leq 5$ for $1 < c < (1 + \sqrt{5})/2 = 1.61\ldots$. Finally, Tolev [214] and Zhai [253] have studied systems of inequalities of the form (5.7).

Several authors [1, 2, 30, 31] have studied variants of Goldbach's problem, suggested by results about additive inequalities. For example, Arkhipov, Chen, and Chubarikov [2] proved that if λ_1/λ_2 is an algebraic irrationality, then all but $O(x^{2/3+\varepsilon})$ positive integers $n \leq x$ can be represented in the form

$$[\lambda_1 p_1] + [\lambda_2 p_2] = n,$$

where p_1, p_2 are primes.

6 A new path: arithmetic progressions of primes

Finally, we should say a few words about the astonishing result of Green and Tao [64] on the existence of arbitrarily long arithmetic progressions of prime numbers. They deduce the existence of such arithmetic progressions from a generalization of a celebrated theorem of Szemerédi [209, 210], which is itself a deep result in combinatorial number theory. Let $\mathcal{A}$ be a set of positive integers with *positive upper density*, that is,

$$\delta(\mathcal{A}) = \limsup_{N\to\infty} \frac{\#\{n \in \mathcal{A} : n \leq N\}}{N} > 0.$$

In its original, most basic form, Szemerédi's theorem asserts that such a set $\mathcal{A}$ contains an arithmetic progression of length k for all integers $k \geq 3$. From this basic statement, Green and Tao deduce the following more general result.

Theorem 9 (Szemerédi's theorem for pseudorandom measures). *Let $\delta \in (0, 1]$ be a fixed real number, let $k \geq 3$ be a fixed integer, and let N be a large prime. Suppose that ν is a "k-pseudorandom measure*[8]*" on $\mathbb{Z}_N = (\mathbb{Z}/N\mathbb{Z})$ and $f : \mathbb{Z}_N \to [0, \infty)$ is a function satisfying*

$$0 \leq f(x) \leq \nu(x) \qquad \text{for all } x \in \mathbb{Z}_N \tag{6.1}$$

and

$$\sum_{x\in\mathbb{Z}_N} f(x) \geq \delta N.$$

[8] A k-pseudorandom measure on $\mathbb{Z}_N$ is a non-negative function on $\mathbb{Z}_N$ whose average over $\mathbb{Z}_N$ is close to 1 and which is subject to a couple of additional constraints that are too technical to state here. See [64] for details.

Then

$$\sum_{x\in\mathbb{Z}_N}\sum_{r\in\mathbb{Z}_N} f(x)f(x+r)\dots f(x+(k-1)r) \gg N^2, \tag{6.2}$$

the implied constant depending at most on δ and k.

To relate this result to the version of Szemerédi's theorem stated earlier, consider the case where $\nu(x) = 1$ for all x (this is a k-pseudorandom measure) and $f(x)$ is the characteristic function of the set $\mathcal{A}_N = \mathcal{A} \cap [1, N]$ considered as a subset of $\mathbb{Z}_N$. Then the left side of (6.2) counts (essentially) the k-term arithmetic progressions in the set $\mathcal{A}_N$ (the majority of which are also k-term arithmetic progressions in $\mathcal{A} \cap \mathbb{Z}$).

To derive the result on arithmetic progressions of primes, Green and Tao take $f(x)$ to be a function which, in some sense (see [64] for details), approximates the characteristic function of the primes in the interval $[c_1N, c_2N]$, where $0 < c_1 < c_2 < 1$ are suitable constants. Then they construct a pseudorandom measure $\nu(x)$ such that (6.1) holds. This leads to the following theorem.

Theorem 10 (Green and Tao, 2004). *Let $k \geq 3$ and let $\mathcal{A}$ be a set of prime numbers such that*

$$\limsup_{N\to\infty} \frac{\#\{n \in \mathcal{A} : n \leq N\}}{\pi(N)} > 0.$$

Then $\mathcal{A}$ contains infinitely many k-term arithmetic progresions. In particular, there are infinitely many k-term arithmetic progresions of prime numbers.

We remark that the infinitude of the k-term progressions of primes is a consequence of (6.2). In fact, using the explicit form of the function $f(x)$ to which they apply Theorem 9, Green and Tao establish the existence of $\gg N^2(\log N)^{-k}$ k-term progressions within $\mathcal{A} \cap [1, N]$.

Several other interesing results are announced in [64]. For example, one of them asserts that there are infinitely many progressions of primes $p_1, \dots, p_k$ such that each $p_i + 2$ is a P_2-number (a proof of this result in the case $k = 3$ is presented in [65]).

Conclusion. With this, our survey comes to a close. We tried to describe the central problems and the main directions of research in the additive theory of prime numbers and to introduce the reader to the classical methods. Complete success in such an undertaking is perhaps an impossibility, but hopefully we have been able to paint a representative picture of the current state of the subject and to motivate the reader to seek more information from the literature. Maybe some of our readers will one day join the ranks of the number theorists trying to turn the great conjectures mentioned above into beautiful theorems!

Acknowledgements. This paper was written while the first author enjoyed the benefits of postdoctoral positions at the University of Toronto and at the University of Texas at Austin. He would like to take this opportunity to express his gratitude to these institutions for their support. The second author was supported by Plovdiv University Scientific Fund grant 03-MM-35. Last but not least, the authors would like to thank Professors J. Friedlander and D.R. Heath-Brown for several valuable discussions over the years and for some useful comments about the preliminary version of the survey.

References

[1] G. I. Arhipov, K. Buriev, and V. N. Chubarikov, *On the exceptional set in the generalized binary Goldbach problem*, Dokl. Ross. Akad. Nauk **365** (1999), 151–153, in Russian.

[2] G. I. Arhipov, J. Y. Chen, and V. N. Chubarikov, *On the cardinality of an exceptional set in a binary additive problem of the Goldbach type*, in "Proceedings of the Session in Analytic Number Theory and Diophantine Equations", Bonner Math. Schriften **360**, Bonn, 2003.

[3] G. I. Arhipov and V. N. Chubarikov, *On the number of summands in Vinogradov's additive problem and its generalizations*, in "Modern Problems of Number Theory and its Applications: Current Problems", vol. 1, Moscow, 2002, pp. 5–38, in Russian.

[4] G. I. Arhipov, V. N. Chubarikov, and A. A. Karatsuba, *Theory of Multiple Trigonometric Sums*, Nauka, 1987, in Russian.

[5] A. Baker, *On some diophantine inequalities involving primes*, J. Reine Angew. Math. **228** (1967), 166–181.

[6] R. C. Baker and G. Harman, *Diophantine approximation by prime numbers*, J. London Math. Soc. (2) **25** (1982), 201–215.

[7] ———, *The three primes theorem with almost equal summands*, R. Soc. London Philos. Trans. Ser. A **356** (1998), 763–780.

[8] R. C. Baker, G. Harman, and J. Pintz, *The exceptional set for Goldbach's problem in short intervals*, in "Sieve Methods, Exponential Sums and their Applications in Number Theory", Cambridge University Press, 1997, pp. 1–54.

[9] ———, *The difference between consecutive primes. II*, Proc. London Math. Soc. (3) **83** (2001), 532–562.

[10] A. Balog, *On the fractional parts of p^θ*, Arch. Math. (Basel) **40** (1983), 434–440.

[11] ———, *Linear equations in primes*, Mathematika **39** (1992), 367–378.

[12] A. Balog and J. B. Friedlander, *A hybrid of theorems of Vinogradov and Piatetski-Shapiro*, Pacific J. Math. **156** (1992), 45–62.

[13] C. Bauer, *A note on sums of five almost equal prime squares*, Arch. Math. (Basel) **69** (1997), 20–30.

[14] ———, *On the sum of a prime and the kth power of a prime*, Acta Arith. **85** (1998), 99–118.

[15] ———, *On the exceptional set for the sum of a prime and the kth power of a prime*, Studia Sci. Math. Hungar. **35** (1999), 291–330.

[16] C. Bauer, M. C. Liu, and T. Zhan, *On a sum of three prime squares*, J. Number Theory **85** (2000), 336–359.

[17] V. Blomer and J. Brüdern, *A three squares theorem with almost primes*, Bull. London Math. Soc., to appear.

[18] K. D. Boklan, *The asymptotic formula in Waring's problem*, Mathematika **41** (1994), 329–347.

[19] E. Bombieri, *On the large sieve*, Mathematika **12** (1965), 201–225.

[20] ———, *Le grand crible dans le théorie analytique des nombres*, Astérisque **18**, Société Math. France, 1974.

[21] ———, *The asymptotic sieve*, Rend. Accad. Naz. XL (5) **1/2** (1975/76), 243–269.

[22] J. Brüdern, *A sieve approach to the Waring–Goldbach problem. I. Sums of four cubes*, Ann. Sci. École Norm. Sup. (4) **28** (1995), 461–476.

[23] ———, *A sieve approach to the Waring–Goldbach problem. II. On the seven cubes theorem*, Acta Arith. **72** (1995), 211–227.

[24] J. Brüdern and E. Fouvry, *Lagrange's four squares theorem with almost prime variables*, J. Reine Angew. Math. **454** (1994), 59–96.

[25] J. Brüdern and K. Kawada, *Ternary problems in additive prime number theory*, in "Analytic Number Theory", Kluwer Acad. Publ., 2002, pp. 39–91.

[26] J. Brüdern and A. Perelli, *The addition of primes and powers*, Canad. J. Math. **48** (1996), 512–526.

[27] V. Brun, *Le crible d'Eratostène et la théorème de Goldbach*, C. R. Acad. Sci. Paris **168** (1919), 544–546.

[28] R. Brünner, A. Perelli, and J. Pintz *The exceptional set for the sum of a prime and a square*, Acta Math. Hungar. **53** (1989), 347–365.

[29] A. A. Buchstab, *Combinatorial intensification of the sieve method of Eratosthenes*, Uspehi Mat. Nauk **22** (1967), 205–233, in Russian.

[30] K. Buriev, *An additive problem with prime numbers*, Dokl. Akad. Nauk Tadzh. SSR **30** (1987), 686–688, in Russian.

[31] ———, *An exceptional set in the Hardy–Littlewood problem for nonintegral powers*, Mat. Zametki **46** (1989), 127–128, in Russian.

[32] Y. C. Cai, *On a diophantine inequality involving prime numbers*, Acta Math. Sinica **39** (1996), 733–742, in Chinese.

[33] ———, *On a diophantine inequality involving prime numbers. III*, Acta Math. Sinica (N.S.) **15** (1999), 387–394.

[34] J. R. Chen, *On large odd numbers as sum of three almost equal primes*, Sci. Sinica **14** (1965), 1113–1117.

[35] ———, *On the representation of large even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica **16** (1973), 157–176.

[36] J. R. Chen and C. D. Pan, *The exceptional set of Goldbach numbers*, Sci. Sinica **23** (1980), 416–430.

[37] K. K. Choi and A. V. Kumchev, *Quadratic equations with five prime unknowns*, J. Number Theory **107** (2004), 357–367.

[38] ———, *Mean values of Dirichlet polynomials and applications to linear equations with prime variables*, preprint.

[39] K. K. Choi and J. Y. Liu, *Small prime solutions of quadratic equations*, Canad. J. Math. **54** (2002), 71–91.

[40] ———, *Small prime solutions of quadratic equations. II*, Proc. Amer. Math. Soc., to appear.

[41] V. N. Chubarikov, *On simultaneous representation of natural numbers by sums of powers of prime numbers*, Dokl. Akad. Nauk SSSR **286** (1986), 828–831, in Russian.

[42] N. G. Chudakov, *On the density of the sets of even integers which are not representable as a sum of two odd primes*, Izv. Akad. Nauk SSSR Ser. Mat. **2** (1938), 25–40, in Russian.

[43] J. G. van der Corput, *Sur l'hypothèse de Goldbach*, Proc. Akad. Wet. Amsterdam **41** (1938), 76–80.

[44] H. Cramér, *Some theorems concerning prime numbers*, Arkiv för Mat. Astronom. och Fysik **15** (1920), 1–32.

[45] ———, *On the order of magnitude of the difference between consecutive primes*, Acta Arith. **2** (1937), 23–46.

[46] H. Davenport, *On sums of positive integral kth powers*, Proc. R. Soc. London Ser. A **170** (1939), 293–299.

[47] ———, *On Waring's problem for fourth powers*, Ann. of Math. (2) **40** (1939), 731–747.

[48] ———, *On sums of positive integral kth powers*, Amer. J. Math. **64** (1942), 189–198.

[49] ———, *Multiplicative Number Theory*, Third ed. revised by H. L. Montgomery, Springer-Verlag, 2000.

[50] H. Davenport and P. Erdös, *On sums of positive integral kth powers*, Ann. of Math. (2) **40** (1939), 533–536.

[51] J.-M. Deshouillers, G. Effinger, H. te Riele, and D. Zinoviev, *A complete Vinogradov* 3*-primes theorem under the Riemann hypothesis*, Electron. Res. Announc. Amer. Math. Soc. **3** (1997), 99–104, (electronic).

[52] G. Dufner, *Binäres Goldbachproblem in kursen Intervallen. I. Die explizite Formel*, Period. Math. Hungar. **29** (1994), 213–243.

[53] ———, *Binäres Goldbachproblem in kursen Intervallen. II*, Period. Math. Hungar. **30** (1995), 37–60.

[54] T. Estermann, *On Goldbach's problem: Proof that almost all even positive integers are sums of two primes*, Proc. London Math. Soc. (2) **44** (1938), 307–314.

[55] ———, *On Kloosterman's sum*, Mathematika **8** (1961), 83–86.

[56] ———, *A new application of the Hardy–Littlewood–Kloosterman method*, Proc. London Math. Soc. (3) **12** (1962), 425–444.

[57] K. B. Ford, *New estimates for mean values of Weyl sums*, Internat. Math. Res. Notices (1995), 155–171.

[58] J. B. Friedlander and H. Iwaniec, *The polynomial* $X^2 + Y^4$ *captures its primes*, Ann. of Math. (2) **148** (1998), 963–1040.

[59] ———, *Asymptotic sieve for primes*, Ann. of Math. (2) **148** (1998), 1041–1065.

[60] P. X. Gallagher, *Primes and powers of 2*, Invent. Math. **29** (1975), 125–142.

[61] M. Z. Garaev, *On the Waring–Goldbach problem with small noninteger exponents*, Acta Arith. **108** (2003), 297–302.

[62] G. Greaves, *On the representation of a number in the form* $x^2 + y^2 + p^2 + q^2$ *where* p *and* q *are odd primes*, Acta Arith. **29** (1976), 257–274.

[63] ———, *Sieves in Number Theory*, Springer-Verlag, 2001.

[64] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, preprint.

[65] ———, *Restriction theory of Selberg's sieve, with applications*, preprint.

[66] H. Halberstam and H. E. Richert, *Sieve Methods*, Academic Press, 1974.

[67] G. H. Hardy and J. E. Littlewood, *A new solution of Waring's problem*, Quart. J. Math. Oxford **48** (1919), 272–293.

[68] ———, *Some problems of "Partitio Numerorum". I. A new solution of Waring's problem*, Göttingen Nach. (1920), 33–54.

[69] ———, *Some problems of "Partitio Numerorum". III. On the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.

[70] ———, *Some problems of "Partitio Numerorum". IV. The singular series in Waring's problem and the value of the number* $G(k)$, Math. Z. **12** (1922), 161–188.

[71] ———, *Some problems of "Partitio Numerorum". V. A further contribution to the study of Goldbach's problem*, Proc. London Math. Soc. (2) **22** (1923), 46–56.

[72] ———, *Some problems of "Partitio Numerorum". VI. Further researches in Waring's problem*, Math. Z. **23** (1925), 1–37.

[73] G. H. Hardy and S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. (2) **17** (1918), 75–115.

[74] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Fifth ed., Oxford University Press, 1979.

[75] G. Harman, *Trigonometric sums over primes. I*, Mathematika **28** (1981), 249–254.

[76] ———, *On the distribution of $\sqrt{p}$ modulo one*, Mathematika **30** (1983), 104–116.

[77] ———, *Diophantine approximation with a prime and an almost–prime*, J. London Math. Soc. (2) **29** (1984), 13–22.

[78] ———, *Diophantine approximation by prime numbers*, J. London Math. Soc. (2) **44** (1991), 218–226.

[79] ———, *Eratosthenes, Legendre, Vinogradov and beyond (the hidden power of the simplest sieve)*, in "Sieve Methods, Exponential Sums and their Applications in Number Theory", Cambridge University Press, 1997, pp. 161–173.

[80] G. Harman and A. V. Kumchev, *On sums of squares of primes*, Math. Proc. Cambridge Philos. Soc., to appear.

[81] G. Harman and P. A. Lewis, *Gaussian primes in narrow sectors*, Mathematika **48** (2001), 119–135.

[82] C. B. Haselgrove, *Some theorems in the analytic theory of numbers*, J. London Math. Soc. **26** (1951), 273–277.

[83] D. R. Heath-Brown, *Three primes and an almost-prime in arithmetic progression*, J. London Math. Soc. (2) **23** (1981), 396–414.

[84] ———, *Prime numbers in short intervals and a generalized Vaughan identity*, Canad. J. Math. **34** (1982), 1365–1377.

[85] ———, *Cubic forms in ten variables*, Proc. London Math. Soc. (3) **47** (1983), 225–257.

[86] ———, *The number of primes in a short interval*, J. Reine Angew. Math. **389** (1988), 22–63.

[87] ———, *A new form of the circle method, and its application to quadratic forms*, J. Reine Angew. Math. **481** (1996), 149–206.

[88] ———, *The circle method and diagonal cubic forms*, R. Soc. London Philos. Trans. Ser. A **356** (1998), 673–699.

[89] ———, *Primes represented by $x^3 + 2y^3$*, Acta Math. **186** (2001), 1–84.

[90] ———, *Lectures on sieves*, in "Proceedings of the Session in Analytic Number Theory and Diophantine Equations", Bonner Math. Schriften **360**, Bonn, 2003.

[91] D. R. Heath-Brown and H. Iwaniec, *On the difference between consecutive primes*, Invent. Math. **55** (1979), 49–69.

[92] D. R. Heath-Brown and B. Z. Moroz, *Primes represented by binary cubic forms*, Proc. London Math. Soc. (3) **84** (2002), 257–288.

[93] D. R. Heath-Brown and J.-C. Puchta, *Integers represented as a sum of primes and powers of two*, Asian J. Math. **6** (2002), 535–565.

[94] D. R. Heath-Brown and D. I. Tolev, *Lagrange's four squares theorem with one prime and three almost-prime variables*, J. Reine Angew. Math. **558** (2003), 159–224.

[95] D. Hilbert, *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl nter Potenzen (Waringsche Problem)*, Math. Ann. **67** (1909), 281–300.

[96] G. Hoheisel, *Primzahlprobleme in der Analysis*, Sitz. Preuss. Akas. Wiss. **2** (1930), 1–13.

[97] C. Hooley, *On the representation of a number as the sum of two squares and a prime*, Acta Math. **97** (1957), 189–210.

[98] ———, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge University Press, 1976.

[99] ———, *On Waring's problem*, Acta Math. **157** (1986), 49–97.

[100] L. K. Hua, *Some results in the additive prime number theory*, Quart. J. Math. Oxford **9** (1938), 68–80.

[101] ———, *An improvement of Vinogradov's mean-value theorem and several applications*, Quart. J. Math. Oxford **20** (1949), 48–61.

[102] ———, *Additive Theory of Prime Numbers*, American Mathematical Society, 1965.

[103] A. Ivic, *The Riemann Zeta-function*, John Wiley & Sons, 1985.

[104] H. Iwaniec, *Almost-primes represented by quadratic polynomials*, Invent. Math. **47** (1978), 171–188.

[105] ———, *Rosser's sieve*, Acta Arith. **36** (1980), 171–202.

[106] ———, *A new form of the error term in the linear sieve*, Acta Arith. **37** (1980), 307–320.

[107] H. Iwaniec and M. Jutila, *Primes in short intervals*, Ark. Mat. **17** (1979), 167–176.

[108] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society, 2004.

[109] C. H. Jia, *The three primes theorem over short intervals*, Acta Math. Sinica **32** (1989), 464–473, in Chinese.

[110] ———, *Three primes theorem in a short interval. VII*, Acta Math. Sinica (N.S.) **10** (1994), 369–387.

[111] ———, *Goldbach numbers in a short interval. I*, Sci. China Ser. A **38** (1995), 385–406.

[112] ———, *Goldbach numbers in a short interval. II*, Sci. China Ser. A **38** (1995), 513–523.

[113] ———, *On the Piatetski-Shapiro–Vinogradov theorem*, Acta Arith. **73** (1995), 1–28.

[114] ———, *Almost all short intervals containing prime numbers*, Acta Arith. **76** (1996), 21–84.

[115] ———, *On the exceptional set of Goldbach numbers in a short interval*, Acta Arith. **77** (1996), 207–287.

[116] A. A. Karatsuba, *Basic Analytic Number Theory*, translated from the second Russian edition, Springer-Verlag, 1993.

[117] A. A. Karatsuba and S. M. Voronin, *The Riemann Zeta-function*, Walter de Gruyter, 1992.

[118] K. Kawada, *Note on the sum of cubes of primes and an almost prime*, Arch. Math. (Basel) **69** (1997), 13–19.

[119] ———, *On sums of seven cubes of almost primes*, preprint.

[120] K. Kawada and T. D. Wooley, *Sums of fourth powers and related topics*, J. Reine Angew. Math. **512** (1999), 173–223.

[121] ———, *On the Waring–Goldbach problem for fourth and fifth powers*, Proc. London Math. Soc. (3) **83** (2001), 1–50.

[122] H. D. Kloosterman, *On the representation of numbers in the form* $ax^2 + by^2 + cz^2 + dt^2$, Acta Math. **49** (1926), 407–464.

[123] N. M. Korobov, *Estimates of trigonometric sums and their applications*, Uspehi Mat. Nauk **13** (1958), 185–192, in Russian.

[124] P. Kuhn, *Zur Viggo Brun'schen Siebmethode. I*, Norske Vid. Selsk. Forh. Trondhjem **14** (1941), 145–148.

[125] A. V. Kumchev, *A diophantine inequality involving prime powers*, Acta Arith. **89** (1999), 311–330.

[126] ———, *On the Waring–Goldbach problem: Exceptional sets for sums of cubes and higher powers*, Canad. J. Math., to appear.

[127] ———, *On the Waring–Goldbach problem for seventh powers*, Proc. Amer. Math. Soc., to appear.

[128] ———, *On Weyl sums over primes and almost primes*, preprint.

[129] A. V. Kumchev and M. B. S. Laporta, *On a binary diophantine inequality involving prime powers*, in "Number Theory for the Millennium", vol. 2, AK Peters, 2002, pp. 307–329.

[130] A. V. Kumchev and T. Nedeva, *On an equation with prime numbers*, Acta Arith. **83** (1998), 117–126.

[131] A. Languasco, *On the exceptional set of Goldbach's problem in short intervals*, Monatsh. Math. **141** (2004), 147–169.

[132] ———, *On the exceptional set of Hardy–Littlewood's numbers in short intervals*, Tsukuba J. Math. **28** (2004), 169–191.

[133] M. B. S. Laporta, *On a binary diophantine inequality involving prime numbers*, Acta Math. Hungar. **83** (1999), 179–187.

[134] M. C. Leung and M. C. Liu, *On generalized quadratic equations in three prime variables*, Monatsh. Math. **115** (1993), 133–169.

[135] H. Z. Li, *Goldbach numbers in short intervals*, Sci. China Ser. A **38** (1995), 641–652.

[136] ———, *The exceptional set of Goldbach numbers. II*, Acta Arith. **92** (2000), 71–88.

[137] ———, *The number of powers of 2 in representation of large even integers by sums of such powers and of two primes*, Acta Arith. **92** (2000), 229–237.

[138] ———, *The number of powers of 2 in representation of large even integers by sums of such powers and of two primes. II*, Acta Arith. **96** (2001), 369–379.

[139] ———, *Small prime solutions of linear ternary equations*, Acta Arith. **98** (2001), 293–309.

[140] Yu. V. Linnik, *The large sieve*, Dokl. Akad. Nauk SSSR **30** (1941), 292–294, in Russian.

[141] ———, *On the representation of large numbers as sums of seven cubes*, Mat. Sbornik N.S. **12** (1943), 218–224, in Russian.

[142] ———, *Prime numbers with powers of two*, Trudy Mat. Inst. Steklov **38** (1951), 152–169, in Russian.

[143] ———, *Some conditional theorems concerning the binary Goldbach problem*, Izv. Akad. Nauk SSSR Ser. Mat. **16** (1952), 503–520, in Russian.

[144] ———, *Addition of prime numbers with powers of one and the same number*, Mat. Sbornik N.S. **32** (1953), 3–60, in Russian.

[145] ———, *An asymptotic formula in the Hardy–Littlewood additive problem*, Izv. Akad. Nauk SSSR Ser. Mat. **24** (1960), 629–706.

[146] ———, *The Dispersion Method in Binary Additive Problems*, American Mathematical Society, 1963.

[147] J. Y. Liu, *On Lagrange's theorem with prime variables*, Quart. J. Math. Oxford (2) **54** (2003), 453–462.

[148] J. Y. Liu and M. C. Liu, *Representations of even integers as sums of squares of primes and powers of 2*, J. Number Theory **83** (2000), 202–225.

[149] ———, *The exceptional set in the four prime squares problem*, Illinois J. Math. **44** (2000), 272–293.

[150] J. Y. Liu, M. C. Liu, and T. Wang, *The number of powers of 2 in an representation of large even integers. I*, Sci. China Ser. A **41** (1998), 386–398.

[151] ———, *The number of powers of 2 in an representation of large even integers. II*, Sci. China Ser. A **41** (1998), 1255–1271.

[152] ———, *On the almost Goldbach problem of Linnik*, J. Théor. Nombres Bordeaux **11** (1999), 133–147.

[153] J. Y. Liu, M. C. Liu, and T. Zhan, *Squares of primes and powers of 2*, Monatsh. Math. **128** (1999), 283–313.

[154] ———, *Squares of primes and powers of 2. II*, J. Number Theory **92** (2002), 99–116.

[155] J. Y. Liu, T. D. Wooley, and G. Yu, *The quadratic Waring–Goldbach problem*, J. Number Theory **107** (2004), 298–321.

[156] J. Y. Liu and T. Zhan, *On sums of five almost equal prime squares*, Acta Arith. **77** (1996), 369–383.

[157] ———, *On a theorem of Hua*, Arch. Math. (Basel) **69** (1997), 375–390.

[158] ———, *Hua's theorem on prime squares in short intervals*, Acta Math. Sinica (N.S.) **16** (2000), 669–690.

[159] ———, *Distribution of integers that are sums of three squares of primes*, Acta Arith. **98** (2001), 207–228.

[160] ———, *An iterative method in the Waring–Goldbach problem*, preprint.

[161] M. C. Liu and K. M. Tsang, *Small prime solutions of some additive equations*, Monatsh. Math. **111** (1991), 147–169.

[162] ———, *Small prime solutions of linear equations*, in "Théorie de nombres", Walter de Gruyter, 1989, pp. 595–624.

[163] M. C. Liu and T. Z. Wang, *On the Vinogradov bound in the three primes Goldbach conjecture*, Acta Arith. **105** (2002), 133-175.

[164] S. T. Lou and Q. Yao, *The exceptional set of Goldbach numbers in a short interval*, Acta Math. Sinica **24** (1981), 269–282, in Chinese.

[165] H. Maier, *Small differences between prime numbers*, Michigan Math. J. **35** (1988), 323–344.

[166] R. J. Miech, *On the equation* $n = p + x^2$, Trans. Amer. Math. Soc. **130** (1968), 494–512.

[167] H. Mikawa, *On the exceptional set in Goldbach's problem*, Tsukuba J. Math. **16** (1992), 513–543.

[168] ———, *On the sum of a prime and a square*, Tsukuba J. Math. **17** (1993), 299–310.

[169] ———, *On the sum of three squares of primes*, in "Analytic Number Theory", Cambridge University Press, 1997, pp. 253–264.

[170] D. A. Mitkin, *The number of terms in the Hilbert-Kamke problem in prime numbers*, Diskret. Mat. **4** (1992), 149–158, in Russian.

[171] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Springer–Verlag, 1971.

[172] ———, *The analytic principal of the large sieve*, Bull. Amer. Math. Soc. **84** (1978), 547–567.

[173] H. L. Montgomery and R. C. Vaughan, *The exceptional set in Goldbach's problem*, Acta Arith. **27** (1975), 353–370.

[174] Y. Motohashi, *Sieve Methods and Prime Number Theory*, Tata Institute for Fundamental Research, 1983.

[175] M. B. Nathanson, *Additive Number Theory. The Classical Bases*, Springer-Verlag, 1996.

[176] A. Page, *On the number of primes in an arithmetic progression*, Proc. London Math. Soc. (2) **39** (1935), 116–141.

[177] C. B. Pan and C. D. Pan, *On estimations of trigonometric sums over primes in short intervals. II*, Sci. China Ser. A **32** (1989), 641–653.

[178] ———, *Goldbach Conjecture*, Science Press, 1992.

[179] T. P. Peneva, *On the ternary Goldbach problem with primes p_i such that $p_i + 2$ are almost-prime*, Acta Math. Hungar. **86** (2000), 305–318.

[180] ———, *On the exceptional set for Goldbach's problem in short intervals*, Monatsh. Math. **132** (2001), 49–65; Corrigendum: ibid. **141** (2004), 209–217.

[181] ———, *An additive problem with Piatetski-Shapiro primes and almost-primes*, Monatsh. Math. **140** (2003), 119–133.

[182] A. Perelli and J. Pintz, *On the exceptional set for Goldbach's problem in short intervals*, J. London Math. Soc. (2) **47** (1993), 41–49.

[183] A. Perelli and A. Zaccagnini, *On the sum of a prime and a k–th power*, Izv. Ross. Akad Nauk Ser. Math. **59** (1995), 185–200.

[184] I. I. Piatetski-Shapiro, *On a variant of Waring–Goldbach's problem*, Mat. Sbornik N.S. **30** (1952), 105–120, in Russian.

[185] ———, *On the distribution of prime numbers in sequences of the form $[f(n)]$*, Mat. Sbornik N.S. **33** (1953), 559–566, in Russian.

[186] J. Pintz, *Explicit formulas and the exceptional set in Goldbach's problem*, lecture at the CNTA VIII meeting in Toronto, June 20–25, 2004.

[187] J. Pintz and I. Z. Ruzsa, *On Linnik's approximation to Goldbach's problem. I*, Acta Arith. **109** (2003), 169–194.

[188] ———, *On Linnik's approximation to Goldbach's problem. II*, preprint.

[189] V. A. Plaksin, *An asymptotic formula for the number of solutions of an equation with primes*, Izv. Akad. Nauk SSSR Ser. Math. **45** (1981), 321–397, in Russian.

[190] I. V. Polyakov, *Addition of a prime number and the square of an integer*, Mat. Zametki **47** (1990), 90–99, in Russian.

[191] K. Prachar, *Primzahlverteilung*, Springer–Verlag, 1957.

[192] K. Ramachandra, *On the number of Goldbach numbers in small intervals*, J. Indian Math. Soc. (N.S.) **37** (1973), 157–170.

[193] O. Ramaré, *On Snirel'man's constant*, Ann. Scuola Norm. Sup. Pisa (4) **22** (1995), 645–706.

[194] X. Ren, *The Waring–Goldbach problem for cubes*, Acta Arith. **94** (2000), 287–301.

[195] A. Rényi, *On the representation of an even number as the sum of a single prime and a single almost-prime number*, Dokl. Akad. Nauk SSSR **56** (1947), 455–458, in Russian.

[196] H.-E. Richert, *Selberg's sieve with weights*, Mathematika **16** (1969), 1-22.

[197] G. F. B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monatsber. Berliner Akad., 1859.

[198] J. Rivat and P. Sargos, *Nombres premiers de la forme* $\lfloor n^c \rfloor$, Canad. J. Math. **53** (2001), 414–433.

[199] J. Rivat and J. Wu, *Prime numbers of the form* $[n^c]$, Glasgow Math. J. **43** (2001), 237–254.

[200] K. F. Roth, *On Waring's problem for cubes*, Proc. London Math, Soc. (2) **53** (1951), 268–279.

[201] L. G. Schnirelmann, *Über additive Eigenschaften von Zahlen*, Math. Ann. **107** (1932/33), 649–690.

[202] W. Schwarz, *Zur Darstellun von Zahlen durch Summen von Primzahlpotenzen*, J. Reine Angew. Math. **206** (1961), 78–112.

[203] ———, *Über die Lösbarkeit gewisser Ungleichungen durch Primzahlen*, J. Reine Angew. Math. **212** (1963), 150–157.

[204] A. Selberg, *On an elementary method in the theory of primes*, Norske Vid. Selsk. Forh. Trondhjem **19** (1947), 64–67.

[205] ———, *Collected Papers*, vol. 1, Springer-Verlag, 1989.

[206] ———, *Collected Papers*, vol. 2, Springer-Verlag, 1991.

[207] P. Shields, *Some applications of the sieve methods in number theory*, Ph.D. thesis, University of Wales, 1979.

[208] C. L. Siegel, *Über die Classenzahl quadratischer Körper*, Acta Arith. **1** (1935), 83–86.

[209] E. Szemerédi, *On sets of integers containing no four elements in arithmetic progression*, Acta Math. Acad. Sci. Hungar. **20** (1969), 89–104.

[210] ———, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 299–345.

[211] K. Thanigasalam, *Improvement on Davenport's iterative method and new results in additive number theory. III*, Acta Arith. **48** (1987), 97–116.

[212] E. C. Titchmarsh, *The Theory of the Riemann Zeta-function*, Second ed. revised by D. R. Heath-Brown, Oxford University Press, 1986.

[213] D. I. Tolev, *On a diophantine inequality involving prime numbers*, Acta Arith. **61** (1992), 289–306.

[214] ———, *On a system of two diophantine inequalities with prime numbers*, Acta Arith. **69** (1995), 387–400.

[215] ———, *Arithmetic progressions of prime–almost-prime twins*, Acta Arith. **88** (1999), 67–98.

[216] ———, *Additive problems with prime numbers of special type*, Acta Arith. **96** (2000), 53–88; Corrigendum: ibid. **105** (2002), 205.

[217] ———, *Representations of large integers as sums of two primes of special type*, in "Algebraic Number Theory and Diophantine Analysis", Walter de Gruyter, 2000, pp. 485–495.

[218] ———, *Lagrange's four squares theorem with variables of special type*, in "Proceedings of the Session in Analytic Number Theory and Diophantine Equations", Bonner Math. Schriften **360**, Bonn, 2003.

[219] ———, *On the exceptional set of Lagrange's equation with three prime and one almost-prime variables*, preprint.

[220] R. C. Vaughan, *On Goldbach's problem*, Acta Arith. **22** (1972), 21–48.

[221] ———, *Diophantine approximation by prime numbers. I*, Proc. London Math. Soc. (3) **28** (1974), 373–384.

[222] ———, *Diophantine approximation by prime numbers. II*, Proc. London Math. Soc. (3) **28** (1974), 385–401.

[223] ———, *Mean value theorems in prime number theory*, J. London Math. Soc. (2) **10** (1975), 153–162.

[224] ———, *Diophantine approximation by prime numbers. III*, Proc. London Math. Soc. (3) **33** (1976), 177–192.

[225] ———, *Sommes trigonométriques sure les nombres premiers*, C. R. Acad. Sci. Paris Sér. A **285** (1977), 981–983.

[226] ———, *On Waring's problem for cubes*, J. Reine Angew. Math. **365** (1986), 122–170.

[227] ———, *On Waring's problem for smaller exponents. II*, Mathematika **33** (1986), 6–22.

[228] ———, *The Hardy–Littlewood Method*, Second ed., Cambridge University Press, 1997.

[229] R. C. Vaughan and T. D. Wooley, *Further improvements in Waring's problem*, Acta Math. **174** (1995), 147–240.

[230] ———, *Further improvements in Waring's problem. II. Sixth powers*, Duke Math. J. **76** (1994), 683–710.

[231] ———, *Further improvements in Waring's problem. III. Eighth powers*, Roy. Soc. London Philos. Trans. Ser. A **345** (1993), 385–396.

[232] ———, *Further improvements in Waring's problem. IV. Higher powers*, Acta Arith. **94** (2000), 203–285.

[233] ———, *Waring's problem: a survey*, in "Number Theory for the Millennium", vol. 3, AK Peters, 2002, pp. 301–340.

[234] A. I. Vinogradov, *The density hypothesis for Dirichlet L-series*, Izv. Akad. Nauk SSSR Ser. Mat. **29** (1965), 903–934; Corrigendum: ibid. **30** (1966), 719–720, in Russian.

[235] ———, *The binary Hardy–Littlewood problem*, Acta Arith. **46** (1985), 33–56, in Russian.

[236] I. M. Vinogradov, *Representation of an odd number as the sum of three primes*, Dokl. Akad. Nauk SSSR **15** (1937), 291–294, in Russian.

[237] ———, *Some theorems concerning the theory of primes*, Mat. Sbornik N.S. **2** (1937), 179–195, in Russian.

[238] ———, *The Method of Trigonometrical Sums in the Theory of Numbers*, Trudy Mat. Inst. Steklov **23** (1947), in Russian.

[239] ———, *A new estimate for* $\zeta(1+it)$, Izv. Akad. Nauk SSSR Ser. Mat. **22** (1958), 161–164, in Russian.

[240] ———, *On an upper bound for* $G(n)$, Izv. Akad. Nauk SSSR Ser. Mat. **23** (1959), 637–642, in Russian.

[241] ———, *Special Variants of the Method of Trigonometric Sums*, Nauka, 1976, in Russian.

[242] T. Z. Wang, *On Linnik's almost Goldbach theorem*, Sci. China Ser. A **42** (1999), 1155–1172.

[243] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 204–207.

[244] E. Wirsing, *Thin subbases*, Analysis **6** (1986), 285–308.

[245] T. D. Wooley, *Large improvements in Waring's problem*, Ann. of Math. (2) **135** (1992), 131–164.

[246] ———, *On Vinogradov's mean value theorem*, Mathematika **39** (1992), 379–399.

[247] ———, *New estimates for Weyl sums*, Quart. J. Math. Oxford (2) **46** (1995), 119–127.

[248] ———, *Slim exceptional sets for sums of cubes*, Canad. J. Math. **54** (2002), 417–448.

[249] ———, *Slim exceptional sets for sums of four squares*, Proc. London Math. Soc. (3) **85** (2002), 1–21.

[250] Q. Yao, *The exceptional set of Goldbach numbers in a short interval*, Acta Math. Sinica **25** (1982), 315–322.

[251] A. Zaccagnini, *On the exceptional set for the sum of a prime and kth power*, Mathematika **39** (1992), 400–421.

[252] ———, *A note on the sum of a prime and a polynomial*, Quart. J. Math. Oxford (2) **52** (2001), 519–524.

[253] W. Zhai, *On a system of two diophantine inequalities with prime numbers*, Acta Arith. **92** (2000), 31–46.

[254] T. Zhan, *On the representation of large odd integer as a sum of three almost equal primes*, Acta Math. Sinica (N.S.) **7** (1991), 259–272.

Department of Mathematics, 1 University Station, C1200, The University of Texas at Austin, Austin, TX 78712, U.S.A.

E-mail: kumchev@math.utexas.edu

Department of Mathematics, Plovdiv University "P. Hilendarski", 24 Tsar Asen Street, Plovdiv 4000, Bulgaria

E-mail: dtolev@pu.acad.bg